



Universidad Nacional Autónoma de México



Facultad de Ingeniería

Laboratorio de Administración de Redes

Proyecto Final

Profesora: Ing. Sandra Plata Velázquez

Grupo: 01

Integrantes:

- Jimenez Cervantes Angel Mauricio
- Reyes Romero Luis Fernando

Semestre: 2025-2
Fecha de entrega: 05 - mayo - 2025

índice

Introducción	3
Justificación	4
Desarrollo	14
Tabla de Direccionamientos.....	20
Usuarios y Contraseña de la topología	21
Resultados.....	22
Topología	22
Configuración de HTTPS y DNS.....	23
Tabla de enrutamiento.....	25
Ping entre dispositivos finales	27
Asignación de IP's mediante DHCP	30
Demostración del Sitio web personalizado	32
Demostración del Servicio de VoIP	35
Demostración del funcionamiento del servidor de correo.....	36
Demostración del funcionamiento del servidor de ftp.....	37
Demostración de SSH a los routers.....	39
Demostración de telnet a switches	41
Conclusiones	43
Referencias.....	44

Introducción

En la era moderna, la infraestructura tecnológica es esencial para el funcionamiento eficiente de cualquier organización. Las redes de comunicación, que permiten la interconexión de equipos y sistemas, son la columna vertebral de las operaciones diarias en las empresas. Para garantizar un rendimiento óptimo y una conectividad segura, es fundamental contar con un diseño de cableado estructurado adecuado. Este tipo de cableado no solo asegura una red estable y de alta calidad, sino que también permite un fácil mantenimiento, expansión y actualización de la infraestructura tecnológica.

Este trabajo se enfoca en el diseño y desarrollo de un sistema de cableado estructurado para un edificio de oficinas, donde la necesidad de interconectar múltiples equipos de cómputo, dispositivos telefónicos y otros sistemas es primordial hoy en día. Asimismo, el proyecto se orienta en crear una red que pueda soportar las demandas de conectividad y, al mismo tiempo, adaptarse a las necesidades futuras de la organización. Además, se consideró la integración de servicios críticos como voz IP (VoIP), servidores, y conectividad entre diferentes áreas funcionales. Se ha planificado cuidadosamente el direccionamiento IP mediante la técnica de VLSM (Variable Length Subnet Mask), que permite asignar subredes eficientes y escalables según las necesidades específicas de cada segmento de la red. Por ello, la implementación de OSPF en modalidad multiárea asegura un enrutamiento dinámico, escalable y organizado, alineado con una arquitectura jerárquica de red.

La importancia de este proyecto radica en que un cableado estructurado bien planificado y ejecutado proporciona una base sólida para todas las operaciones digitales de la empresa. En primer lugar, permite la transmisión eficiente de datos, lo que es crucial para el intercambio de información y la comunicación interna. En segundo lugar, este tipo de cableado facilita la integración de nuevos equipos o tecnologías sin necesidad de realizar modificaciones costosas. Además, asegura una mayor seguridad de la red, ya que su estructura organizada y estandarizada reduce el riesgo de fallos y facilita la gestión de los dispositivos conectados.

A través de este proyecto, se busca optimizar la infraestructura tecnológica, mejorando su capacidad de respuesta, reduciendo tiempos de inactividad y garantizando que la red sea lo suficientemente flexible para soportar el crecimiento y la evolución de la organización. Asimismo, la correcta implementación del cableado estructurado será un pilar fundamental para la expansión futura de otros servicios y sistemas dentro de la red corporativa, como servidores de correo, DNS, DHCP y aplicaciones web, que se interconectan de manera eficiente, gracias a una base de red sólida.

Justificación

El uso de normas y estándares en proyectos para la infraestructura de una red es crucial para garantizar la calidad, interoperabilidad, escalabilidad y seguridad del sistema. Estas normas aseguran que los componentes del sistema sean compatibles entre sí, cumpliendo con los requisitos mínimos de desempeño y que puedan ser mantenidos o ampliados en el futuro sin problemas. Además, un diseño basado en normas y estándares facilita la resolución de problemas.

Antes de pasar a la justificación del diseño y la configuración de la red es importante identificar los subsistemas del cableado estructurado que es fundamental para nuestro diseño de red. Por ello, un sistema de cableado estructurado es la infraestructura física que permite la transmisión de voz, datos, video y otros servicios de telecomunicaciones, de forma ordenada, flexible y escalable. Su diseño se basa en la integración de varios subsistemas, cada uno con funciones específicas que, en conjunto, garantizan la fiabilidad y el rendimiento de la red. A continuación, se describe de forma integral cada uno de estos subsistemas:

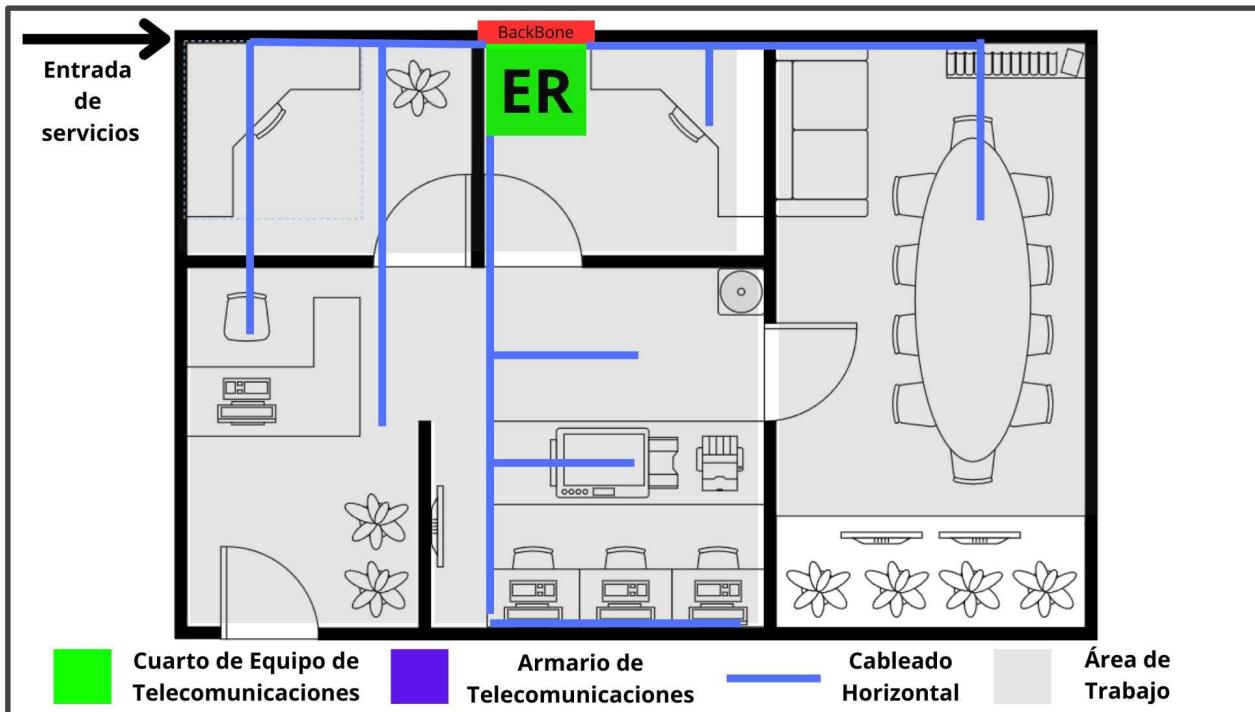
El primer subsistema es el de **La Entrada se Servicios**. Este subsistema representa el punto de ingreso de los servicios de telecomunicaciones externos al edificio. En este lugar se encuentran los puntos de demarcación, donde termina la responsabilidad del proveedor de servicios y comienza la del usuario o del administrador del inmueble. Las instalaciones de entrada incluyen equipos e interfaces que permiten la conexión segura

de los cables procedentes del proveedor, y su ubicación se elige de forma estratégica para evitar interferencias, humedad u otros factores ambientales que pudieran afectar el desempeño del sistema. El siguiente subsistema es el **Cuarto de Equipo de Telecomunicaciones**. Se trata de una sala dedicada exclusivamente a albergar los equipos activos que gestionan el tráfico de datos, voz y vídeo. Dado lo crucial que es el funcionamiento de estos dispositivos, el cuarto de equipo debe contar con un estricto control ambiental, incluyendo sistemas de climatización, control de humedad y protección contra incendios, así como disponer de suficiente espacio para permitir futuras expansiones sin grandes modificaciones en el diseño. Otro componente fundamental es el **Armario de Telecomunicaciones**. Este subsistema, también conocido como closet de telecomunicaciones, se instala en cada piso o zona del edificio para funcionar como nodo de interconexión local. Su función principal es recibir el cableado horizontal que se extiende hacia las áreas de trabajo y conectarlo con el cableado backbone. Es esencial que la ubicación de estos armarios sea central en relación con las áreas que deben servir, de modo que la longitud del cableado horizontal no exceda los 90 metros, cumpliendo así con las normativas vigentes.

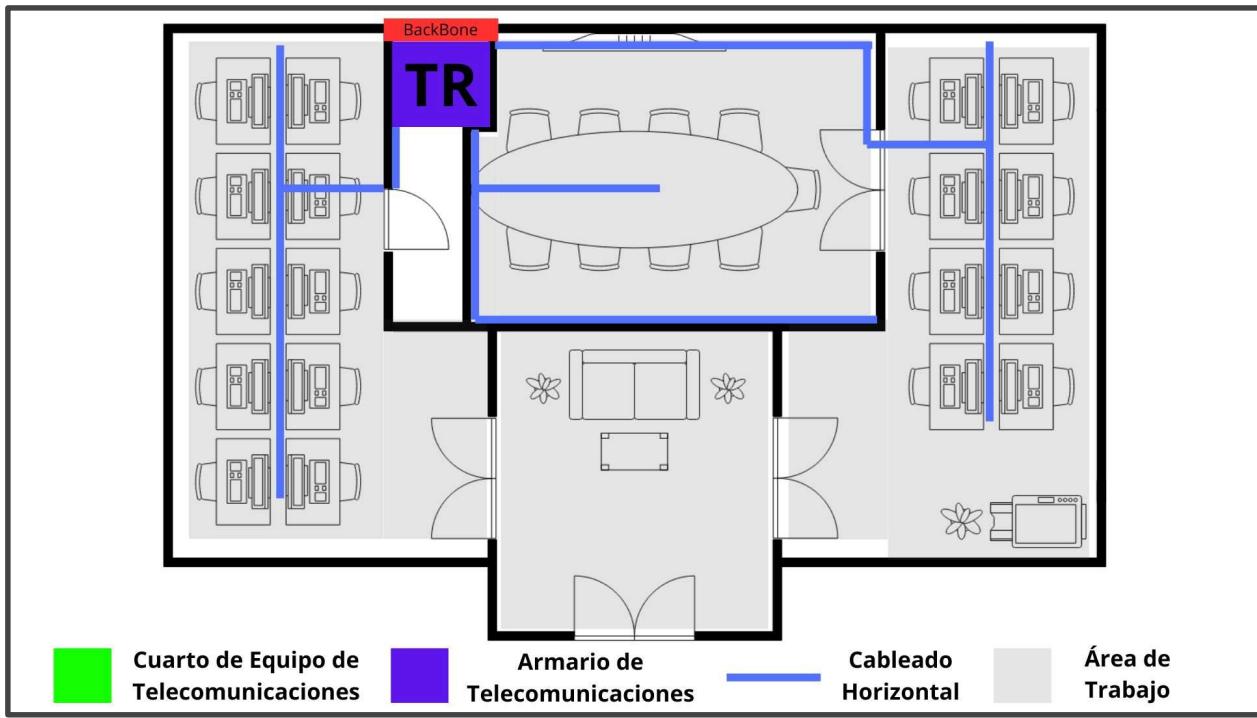
Por otra parte, la función del **Cableado Backbone** es interconectar las instalaciones de entrada, el cuarto de equipo de telecomunicaciones y los armarios de telecomunicaciones, permitiendo el transporte centralizado de grandes volúmenes de datos entre los distintos subsistemas del edificio. Este subsistema suele configurarse en una topología en estrella, en la que un punto central (ubicado en el cuarto de equipo o en un armario central) distribuye la señal a los nodos de cada piso o zona, respetando las distancias máximas que aseguran la calidad de la transmisión. El **Cableado Horizontal** es el subsistema encargado de conectar los armarios de telecomunicaciones con las áreas de trabajo, es decir, el tramo final por el cual la señal llega a los dispositivos del usuario. En esta parte se utilizan principalmente cables de par trenzado (UTP o STP), aunque en entornos que requieran mayores velocidades o ancho de banda se puede recurrir también a la fibra óptica. Finalmente, las **Áreas de Trabajo** comprenden los espacios donde se conectan los dispositivos finales, como computadoras, teléfonos IP, impresoras, cámaras de video, entre otros. Este subsistema define el punto de acceso final a la red, donde se instala el equipo del usuario. Es fundamental que cada área de

trabajo cuente con suficientes puntos de conexión para satisfacer las necesidades de comunicación, y que los cables o patch cords utilizados sean de longitudes cortas, minimizando las pérdidas de señal y asegurando un rendimiento óptimo. Teniendo en cuenta las definiciones de los subsistemas de un cableado estructurado, realizaremos la identificación de estos en un plano. A continuación, presentaremos los subsistemas dentro del plano:

Subsistemas del cableado estructurado para planta 0



Subsistemas del cableado estructurado para planta 1



Justificación del diseño de la topología de red

Para el diseño de nuestra topología tuvimos en cuenta la escalabilidad de la red, asegurándonos de que fuera posible expandirse en un futuro sin afectar su desempeño ni su organización. Para lograrlo, se adoptó el modelo jerárquico de red, el cual proporciona una arquitectura clara, modular y eficiente. Este modelo se divide en tres capas:

- **Capa de acceso:** Capa donde se conectan los dispositivos finales (PCs, teléfonos VoIP).
- **Capa de distribución:** Es la capa que actúa como punto de interconexión entre la capa de acceso y la de núcleo, aplicando políticas de red.
- **Capa núcleo (core):** Es la capa encargada de transportar grandes cantidades de datos rápidamente entre las diferentes partes de la red.

Implementación de OSPF Multiárea

Para el enrutamiento dinámico entre los diferentes segmentos de red, se implementó el protocolo OSPF (Open Shortest Path First) en su modalidad multiárea, dividiendo la red en dos áreas conectadas directamente al área backbone (área 0).

Esta configuración se eligió por las siguientes razones:

- Escalabilidad y eficiencia: el uso de múltiples áreas permite reducir la carga de procesamiento en los routers al limitar la propagación de información de enrutamiento innecesaria a través de toda la red.
- Organización lógica: cada área agrupa redes relacionadas funcionalmente, lo cual facilita la administración y el aislamiento de fallas.
- Cumplimiento con el diseño jerárquico: OSPF multiárea se alinea con el modelo jerárquico de red adoptado, mejorando el control del tráfico interno.

Gracias a esta implementación, la red mantiene una convergencia rápida, rutas optimizadas y una estructura modular lista para futuras expansiones.

Además, OSPF Multiárea tiene grandes ventajas frente a otros protocolos:

- Comparación con RIP (Routing Information Protocol):
 1. OSPF tiene una escalabilidad superior ya que, puede dividir la red en múltiples áreas, mientras que RIP tiene un límite de 15 saltos.
 2. OSPF tiene una convergencia más rápida debido a que detecta y adapta cambios más rápido que RIP.
 3. El uso eficiente del ancho de banda: OSPF solo envía actualizaciones cuando hay cambios, RIP envía todo cada 30 segundos.
 4. Soporte jerárquico: RIP no tiene estructura jerárquica, OSPF sí.
- Comparación con EIGRP (Enhanced Interior Gateway Routing Protocol):
 1. Diseño jerárquico: OSPF multiárea permite un control más fino del tráfico. En cambio, EIGRP no tiene áreas.
 2. Escalabilidad controlada: OSPF puede subdividir grandes redes en áreas; EIGRP escala, pero sin jerarquía formal.

3. Transparencia del cálculo de rutas: OSPF usa SPF (algoritmo de Dijkstra), más transparente que el algoritmo dual de EIGRP.
4. Interoperabilidad: OSPF funciona mejor en entornos multi vendedor.

Asignación de direcciones IP y configuración DHCP

Para la asignación dinámica de direcciones IP, se optó por utilizar el router como servidor DHCP debido a las siguientes razones:

- El router permite definir múltiples pools de direcciones, lo cual es útil para segmentar servicios como VoIP, servidores o usuarios administrativos.
- En el caso del servicio de VoIP, es necesario configurar la opción 150 del protocolo DHCP, que permite proporcionar la IP del servidor TFTP, fundamental para que los teléfonos IP puedan descargar su configuración y firmware automáticamente. Esta opción solo está disponible si el DHCP está alojado en el router.

Durante las primeras fases del proyecto, se identificó que algunos servidores no estaban asignando correctamente los parámetros esenciales del DHCP, como el gateway predeterminado (default-router), por lo que se optó por centralizar esta función en el router para mayor confiabilidad y control. Además, una configuración incorrecta del gateway predeterminado puede tener consecuencias críticas en el funcionamiento de nuestra red como son:

- Los dispositivos no podrán comunicarse con redes fuera de su segmento local, afectando el acceso a Internet o a servidores remotos.
- Aplicaciones como VoIP, correo electrónico o autenticación pueden fallar si requieren acceso a recursos fuera de la red local.
- Si el DNS se encuentra fuera de la subred, los equipos no podrán resolver nombres de dominio correctamente.
- Los administradores no podrán acceder a los equipos desde otras redes para diagnóstico o soporte.
- Una puerta de enlace incorrecta puede causar rutas ineficientes o incluso bucles de red, afectando el rendimiento general.
- Algunos dispositivos podrían tener conectividad y otros no, dificultando la detección de fallos y el soporte técnico.

Por estas razones, se prioriza la centralización del servicio DHCP en el router, asegurando que todos los dispositivos reciban una configuración coherente y confiable, incluyendo el gateway correcto.

Segmentación y organización física

Para mantener una red organizada y con separación lógica de servicios, se implementó un segmento exclusivo para VoIP, conectado mediante un switch independiente. Esta separación no solo evita posibles conflictos o congestión entre servicios, sino que también facilita el crecimiento ordenado del sistema y mejora la administración dentro del rack de comunicaciones ya que, al reducir la competencia por el ancho de banda con otros servicios, se minimiza la latencia, la fluctuación y la pérdida de paquetes, garantizando comunicaciones de voz más estables y claras.

Elección del modelo de router

El modelo de router utilizado fue seleccionado específicamente por ser el único, dentro de la versión de Cisco Packet Tracer empleada en este proyecto, que ofrece compatibilidad total con las funciones necesarias para implementar servicios de VoIP. Esta compatibilidad incluye:

- La creación de pools DHCP avanzados, que permiten incluir la opción 150, indispensable para enviar la dirección IP del servidor TFTP a los teléfonos IP.
- La configuración de dial peers, que son esenciales para definir las rutas de llamadas entre dispositivos y facilitar la comunicación entre distintas subredes VoIP.
- La habilitación del router como gateway de telefonía IP, permitiendo que actúe como controlador de llamadas, dirigiendo y gestionando el tráfico de voz dentro de la red.

La elección de este modelo asegura que todas las funcionalidades requeridas para una solución de VoIP básica puedan ser simuladas y probadas correctamente, garantizando así la viabilidad y funcionalidad de la red propuesta.

Tipos de cableado utilizado

Para garantizar una conectividad adecuada y conforme a las buenas prácticas de diseño de redes, se emplearon distintos tipos de cableado según el tipo de dispositivos interconectados:

- Cables directos (straight-through): Utilizados para conectar dispositivos finales como PCs, teléfonos IP y servidores a los switches. Este tipo de cable permite la comunicación entre dispositivos de diferente tipo y es el más común en conexiones de acceso.
- Cables cruzados: Empleados en las interconexiones entre dispositivos del mismo tipo, como switch-switch o router-switch.
- Cable serial: Utilizado para establecer enlaces punto a punto entre routers ubicados en distintos pisos o segmentos de red, simulando enlaces WAN o troncales entre áreas OSPF.

Conexión dedicada para servidores

De igual manera, se destinó un switch exclusivo para la conexión de los servidores, lo cual proporciona múltiples beneficios a nivel de rendimiento, escalabilidad y organización de la red:

- Al separar físicamente los servidores de otros dispositivos como PCs o teléfonos, se asegura que los puertos del switch estén dedicados exclusivamente a los servicios críticos dentro de la red.
- Esto evita la congestión en switches compartidos, manteniendo un rendimiento óptimo tanto para los servicios como para los usuarios finales.
- El switch dedicado permite añadir nuevos servidores sin afectar la estructura existente, lo cual es ideal en entornos en crecimiento o con proyección de escalabilidad.
- Al concentrar los servidores en un único punto físico, se simplifica la gestión de tráfico, seguridad, mantenimiento y resolución de problemas.

Servicios adicionales: Syslog y NTP

Con el objetivo de fortalecer la administración y el monitoreo de la red, se integraron los servicios de Syslog y NTP (Network Time Protocol) como parte de la infraestructura de red:

- Para el servidor Syslog: Se configuró un servidor Syslog centralizado para recibir y almacenar los mensajes de registro generados por los dispositivos de red. Esta implementación permite:
 - ❖ Monitorear el estado operativo de routers, switches y otros equipos en tiempo real.
 - ❖ Detectar fallas, intentos de acceso no autorizados o comportamientos anómalos de forma más rápida.
- Para el servidor NTP: Se implementó un servidor NTP como fuente de sincronización de hora, permitiendo:
 - ❖ Una sincronización precisa del reloj en todos los dispositivos de red.
 - ❖ Coherencia temporal en los registros Syslog, lo que es crucial para la correlación de eventos y análisis forense.
 - ❖ Reducción de errores en tareas automatizadas que dependen del tiempo, como backups, autenticaciones o tareas programadas.

Seguridad de capa 2 y configuración de puertos

Se implementó el protocolo PortFast en los puertos de acceso para que, al conectar un dispositivo final, estos pasen inmediatamente del estado Blocking al estado Forwarding, acelerando la disponibilidad del puerto sin esperar los 30 segundos típicos del STP.

Además, se configuró Port Security en los switches para limitar la cantidad de dispositivos por puerto, previniendo accesos no autorizados y mejorando la seguridad a nivel físico.

Acceso remoto seguro a dispositivos de red

Para la gestión remota de los dispositivos, se optó por habilitar el acceso mediante SSH (Secure Shell) en los routers, ya que estos manejan información sensible relacionada con la distribución de direcciones IP, rutas estáticas y dinámicas, y parámetros de

servicios críticos como VoIP. SSH proporciona encriptación de extremo a extremo, lo cual garantiza la confidencialidad e integridad de las credenciales y comandos transmitidos.

En cambio, en los switches se habilitó acceso por Telnet, dado que su función se limita principalmente a la interconexión de dispositivos de capa 2, y no almacenan o procesan información crítica. Esto permite una administración básica sin comprometer significativamente la seguridad general de la red. No obstante, se consideró que en un entorno real, el uso de SSH también debería extenderse a los switches para mantener un estándar uniforme de seguridad.

Seguridad de acceso al equipo

Por último, se configuraron contraseñas cifradas de nivel 5 en el modo privilegiado y para los accesos de usuario en los routers y switches. Esto incrementa la seguridad del sistema, ya que evita el acceso no autorizado a la configuración del equipo, protegiendo así la integridad y disponibilidad de la red.

Desarrollo

VLSM para subredes

Planta 0

Segmento 195.231.18.0 / 24

Para poder aplicar VLSM al segmento de red vamos a explicar paso a paso como se lleva a cabo este método. Primero vamos a definir VLSM (Variable Length Subnet Mask) permite dividir una red IP en subredes de distintos tamaños (longitudes de máscara variables), lo que evita desperdiciar direcciones IP.

Paso 1: Ordena las subredes por tamaño (de mayor a menor hosts)

- Administración 20 hosts
- Área Común 10 hosts
- Sala de conferencias 10 hosts
- Red para VoIP 10 hosts
- Recepción 6 host

Paso 2: Calcula el tamaño de cada subred necesaria con la siguiente fórmula:

$$2^n - 2 \geq \text{Número de hosts requeridos}$$

Donde:

- 2^n representa el total de direcciones IP posibles con "n" bits para la parte de host.
- -2 se resta porque:
 - ❖ Una dirección se reserva para la **dirección de red**.
 - ❖ Otra se reserva para la **dirección de broadcast**.

Se debe iniciar desde el segmento 195.231.18.0 para que no haya direcciones desperdiciadas.

Para la primera subred, necesitamos 20 hosts para la parte de administración de la planta 0. Dado que contamos con una máscara de red con el prefijo /24, no es necesario expresar toda la dirección en binario, ya que los primeros tres octetos de la dirección

permanecen constantes debido a la máscara de red. Solo modificaremos el último octeto según el número de hosts requeridos en cada subred.

Entonces tenemos que:

$$2^5 - 2 \geq 20 \Rightarrow 32 - 2 \geq 20 \Rightarrow 30 \geq 20 \text{ (Administración)}$$

$$195.231.18.000|00000 \rightarrow 195.231.18.0/27 \text{ (ID de red)}$$

$$195.231.18.000|00001 \rightarrow 195.231.18.0/27 \text{ (Primera dirección asignable)}$$

$$195.231.18.000|11110 \rightarrow 195.231.18.30/27 \text{ (Última dirección asignable)}$$

$$195.231.18.000|11111 \rightarrow 195.231.18.31/27 \text{ (Broadcast)}$$

Algo que debemos de tomar en cuenta es que la última dirección assignable de una subred se suele reservar para el gateway porque, en muchas configuraciones de red, se emplea la dirección más alta del rango de host disponible para facilitar la administración y la identificación de la puerta de enlace predeterminada. Esta práctica asegura que el gateway se encuentra dentro del bloque de direcciones utilizables, pero al mismo tiempo se distingue como una dirección única y fácilmente localizable en el extremo superior del rango de IPs disponibles, antes de la dirección de broadcast.

Seguimos calculando las subredes de la misma forma.

$$2^4 - 2 \geq 10 \Rightarrow 16 - 2 \geq 10 \Rightarrow 14 \geq 10 \text{ (Área Común)}$$

$$195.231.18.0010|0000 \rightarrow 195.231.18.32/28 \text{ (ID de red)}$$

$$195.231.18.0010|0001 \rightarrow 195.231.18.33/28 \text{ (Primera dirección asignable)}$$

$$195.231.18.0010|1110 \rightarrow 195.231.18.46/28 \text{ (Última dirección asignable)}$$

$$195.231.18.0010|1111 \rightarrow 195.231.18.47/28 \text{ (Broadcast)}$$

$$2^4 - 2 \geq 10 \Rightarrow 16 - 2 \geq 10 \Rightarrow 14 \geq 10 \text{ (Sala de Conferencias)}$$

$$195.231.18.0011|0000 \rightarrow 195.231.18.48/28 \text{ (ID de red)}$$

$$195.231.18.0011|0001 \rightarrow 195.231.18.49/28 \text{ (Primera dirección asignable)}$$

$$195.231.18.0011|1110 \rightarrow 195.231.18.62/28 \text{ (Última dirección asignable)}$$

$$195.231.18.0011|1111 \rightarrow 195.231.18.63/28 \text{ (Broadcast)}$$

$$2^4 - 2 \geq 10 \Rightarrow 16 - 2 \geq 10 \Rightarrow 14 \geq 10 \text{ (Direcciones para VoIP)}$$

195.231.18.0100|0000 → 195.231.18.64/28 (ID de red)

195.231.18.0100|0001 → 195.231.18.65/28 (Primera dirección asignable)

195.231.18.0100|1110 → 195.231.18.78/28 (Última dirección asignable)

195.231.18.0100|1111 → 195.231.18.79/28 (Broadcast)

$$2^3 - 2 \geq 6 \Rightarrow 8 - 2 \geq 6 \Rightarrow 6 \geq 6 \text{ (Recepción)}$$

195.231.18.01010|000 → 195.231.18.80/29 (ID de red)

195.231.18.01010|001 → 195.231.18.81/29 (Primera dirección asignable)

195.231.18.01010|110 → 195.231.18.86/29 (Última dirección asignable)

195.231.18.01010|111 → 195.231.18.87/29 (Broadcast)

Una vez que hayamos calculado todas las subredes, identificando nuestro ID de red, rango assignable, máscara de red, dirección de broadcast y gateway, debemos colocar toda esta información en nuestra tabla de direccionamiento.

Tabla de direccionamiento para la planta 0

Red	Id de Red	Rango Asignable	Gateway	Máscara	Broadcast
AD	195.231.18.0	195.231.18.1 a 195.231.18.30	195.23 1.18.30	255.255.255.224	195.231.18.31
AC	195.231.18.32	195.231.18.33 a 195.231.18.46	195.23 1.18.46	255.255.255.240	195.231.18.47
SC	195.231.18.48	195.231.18.49 a	195.23 1.18.62	255.255.255.240	195.231.18.62

		195.231.18.62			
VP0	195.231.18.64	195.231.18.65 a 195.231.18.78	195.23 1.18.78	255.255.255.240	195.231.18.79
RP	195.231.18.80	195.231.18.81 a 195.231.18.86	195.23 1.18.86	255.255.255.248	195.231.18.87

Planta 1

Segmento 201.10.1.0 / 24

Para la planta 1 es el mismo procedimiento que hicimos en la planta 0, solo que ahora lo que cambia es nuestro segmento de red.

Paso 1: Ordena las subredes por tamaño (de mayor a menor hosts)

- Área de Cubículos Norte 30 hosts
- Área de Cubículos Sur 25 hosts
- Sala de Reuniones 20 hosts
- Red para VoIP 10 hosts

Paso 2: Calcula el tamaño de cada subred necesaria con la siguiente fórmula:

$$2^n - 2 \geq \text{Número de hosts requeridos}$$

Entonces tenemos que:

$$2^5 - 2 \geq 30 \Rightarrow 32 - 2 \geq 30 \Rightarrow 30 \geq 30 \text{ (Área de Cubículos Norte)}$$

$$201.10.1.000|00000 \rightarrow 201.10.1.0/27 \text{ (ID de red)}$$

$$201.10.1.000|00001 \rightarrow 201.10.1.1/27 \text{ (Primera dirección asignable)}$$

$$201.10.1.000|11110 \rightarrow 201.10.1.30/27 \text{ (Última dirección asignable)}$$

$$201.10.1.000|11111 \rightarrow 201.10.1.31/27 \text{ (Broadcast)}$$

$$2^5 - 2 \geq 25 \Rightarrow 32 - 2 \geq 25 \Rightarrow 30 \geq 25 \text{ (Área de Cubículos Sur)}$$

201.10.1.001|00000 → 201.10.1.32/27 (*ID de red*)

201.10.1.001|00001 → 201.10.1.33/27 (*Primera dirección asignable*)

201.10.1.001|11110 → 201.10.1.62/27 (*Última dirección asignable*)

201.10.1.001|11111 → 201.10.1.63/27 (*Broadcast*)

$$2^5 - 2 \geq 20 \Rightarrow 32 - 2 \geq 20 \Rightarrow 30 \geq 20 \text{ (Sala de Reuniones)}$$

201.10.1.010|00000 → 201.10.1.64/27 (*ID de red*)

201.10.1.010|00001 → 201.10.1.65/27 (*Primera dirección asignable*)

201.10.1.010|11110 → 201.10.1.94/27 (*Última dirección asignable*)

201.10.1.010|11111 → 201.10.1.95/27 (*Broadcast*)

$$2^4 - 2 \geq 10 \Rightarrow 16 - 2 \geq 10 \Rightarrow 14 \geq 10 \text{ (Red para VoIP)}$$

201.10.1.0110|0000 → 201.10.1.96/27 (*ID de red*)

201.10.1.0110|0001 → 201.10.1.97/27 (*Primera dirección asignable*)

201.10.1.0110|1110 → 201.10.1.110/27 (*Última dirección asignable*)

201.10.1.010|11111 → 201.10.1.111/27 (*Broadcast*)

De igual manera, una vez identificado nuestro ID de red, rango asignable, máscara de red, dirección de broadcast y gateway, debemos colocar toda esta información en nuestra tabla de direccionamiento.

Tabla de direccionamiento para Piso 1

Red	Id de Red	Rango Asignable	Gateway	Máscara	Broadcast
ACN	201.10.1.0	201.10.1.1 a 201.10.1.30	201.10.1.30	255.255.255.224	201.10.1.31
		201.10.1.33			

ACS	201.10.1.32	a 201.10.1.62	201.10.1.62	255.255.255.224	201.10.1.63
SR	201.10.1.64	201.10.1.65 a 201.10.1.94	201.10.1.94	255.255.255.224	201.10.1.95
VP1	201.10.1.96	201.10.1.97 a 201.10.1.110	201.10.1.110	255.255.255.240	201.10.1.111

WAN

Segmento 192.169.1.0 / 26

Para las conexiones seriales es más sencillo VLSM ya que, solo usamos una red para dos hosts.

- Conexión serial 2 hosts

$$2^4 - 2 \geq 10 \Rightarrow 16 - 2 \geq 10 \Rightarrow 14 \geq 10 \text{ (Conexiones Seriales)}$$

192.169.1.000000|00 → 192.169.1.0/30 (*ID de red*)

192.169.1.000000|01 → 192.169.1.1/30 (*Primera dirección asignable*)

192.169.1.000000|10 → 192.169.1.2/30 (*Última dirección asignable*)

192.169.1.000000|11 → 192.169.1.3/30 (*Broadcast*)

Nuevamente colocamos todos nuestros datos en nuestra tabla de direccionamiento.

Tabla de direccionamiento para las conexiones seriales

Red	Id de Red	Rango Asignable	Gateway	Máscara	Broadcast
WAN	192.169.1.0	192.169.1.1 a 192.169.1.2	-	255.255.255.252	192.169.1.3

Tabla de Direccionamientos

Direccionamientos Piso 0	
Dispositivo	Dirección IP
RouterPiso0	192.169.1.1 195.231.18.30 195.231.18.46 195.231.18.62 195.231.18.78 195.231.18.86
Switch_Piso0_Distribucion	195.231.18.61
Switch_Piso0_Servers	195.231.18.28
Switch_Piso0_Datos	195.231.18.45
Switch_Piso0_VoIP	195.231.18.77
Server HTTPS	195.231.18.29
Server FTP	195.231.18.27
Server NTP/Syslog	195.231.18.20
Controladora_APs	195.231.18.26
AP_Administracion	195.231.18.25
AP_SalaConferencia	195.231.18.22
AP_AreaComun	195.231.18.23
AP_Repcion	195.231.18.24

Direccionamientos Piso 1	
Dispositivo	Dirección IP
RouterPiso1	192.169.1.2 201.10.1.30 201.10.1.62 201.10.1.94 201.10.1.110
Switch_Piso1_Distribucion	201.10.1.29
Switch1_Piso1_Datos	201.10.1.93
Switch2_Piso1_Datos	201.10.1.61
Switch_Piso0_VoIP	201.10.1.109

Usuarios y Contraseña de la topología

Credenciales para Usuario en todos los Routers y Switches	
Username	Password
admin	admin

Password de todos los Router y Switches en modo privilegiado
Admin_AR01

Credenciales para la Controladora de los AP's	
Username	Password
Mauricio	Admin_AR01

Credenciales para las redes inalámbricas	
Recepcion	repcion01
Sala Conferencia	Salaconferencia01
Administracion	AdminAR1
Area Comun	Areacomun01
SalaReuniones	SalaReuniones1

Extensiones de Cada Piso	
Piso 0	Piso 1
54001	64001
54002	64002
54003	64003
54004	64004
	64005
	64006

Credenciales para Usuarios en servidor ftp	
Username	Password
Fernando	redes
Mauricio	redes
Sandra	redes
cisco	cisco

Credenciales para Usuarios en servidor de email	
Dirección	Password
Fernando@gmail.com	redes
Mauricio@gmail.com	redes
Sandra@gmail.com	redes
Admin@gmail.com	redes

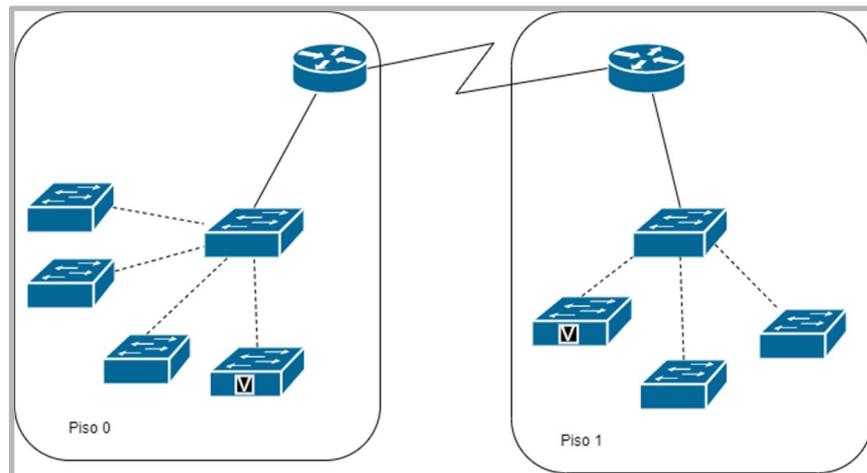
Resultados

En esta sección agregaremos capturas de pantalla de nuestra topología. Se adjunta el link de nuestro repositorio en GitHub para mostrar el avance del proyecto:

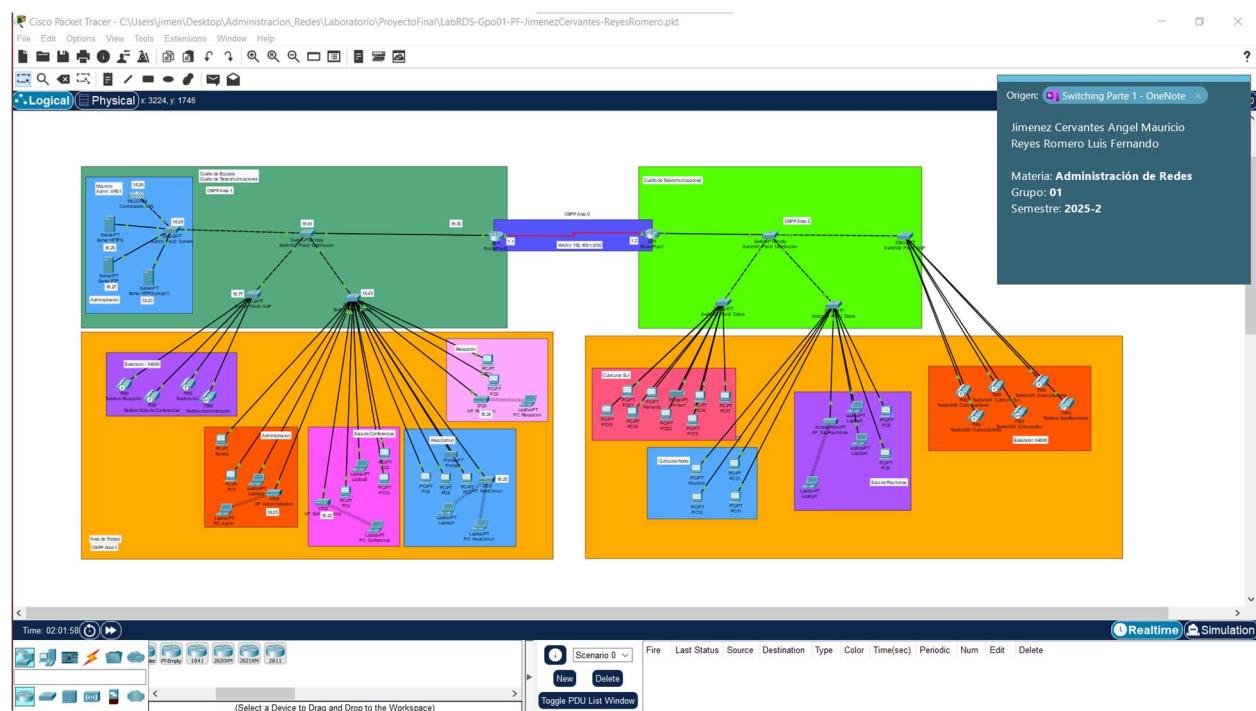
<https://github.com/Mauricio658/ProyectoFinal-LaboratorioAdminRedes.git>

Topología

Diseño de la topología antes de la implementación



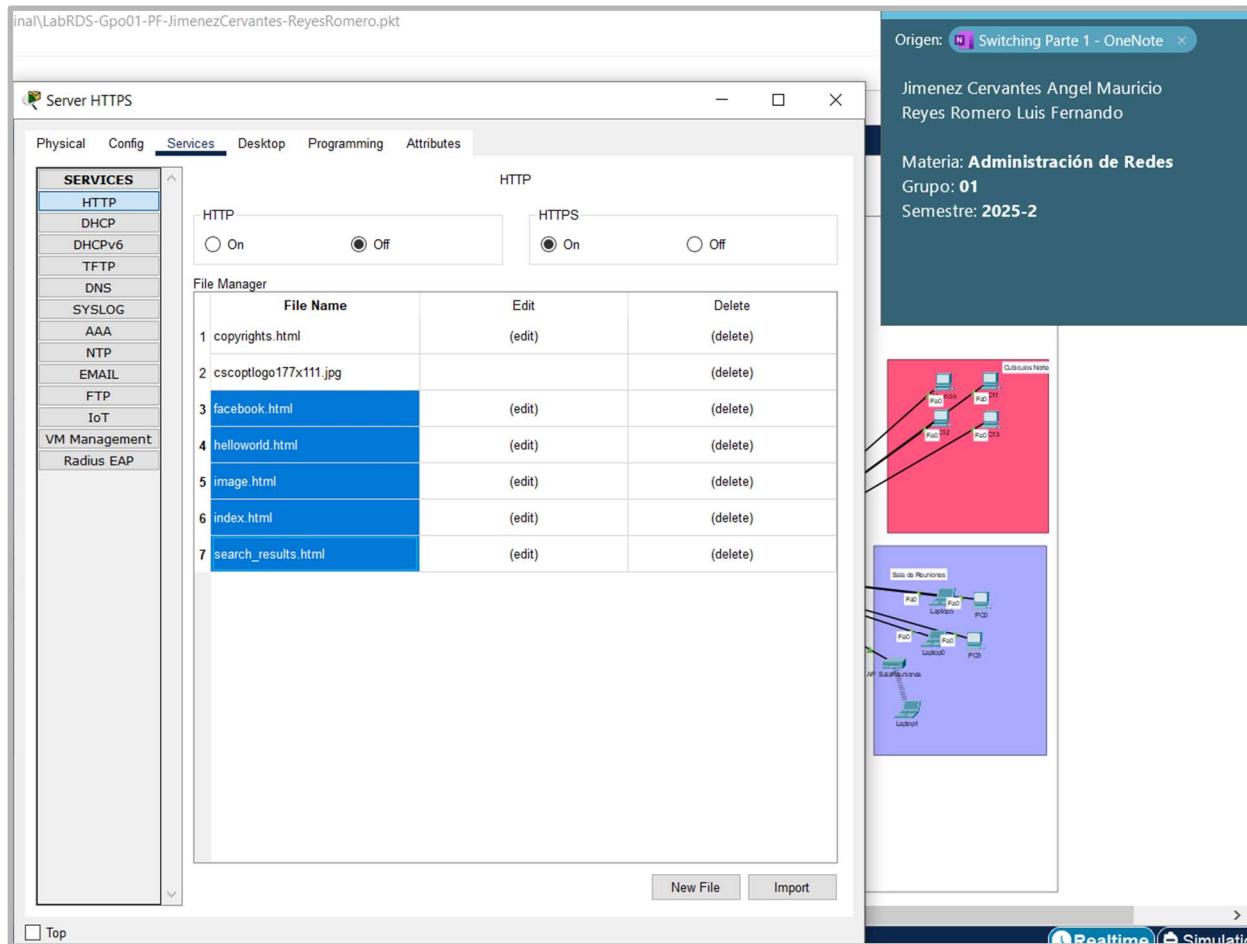
Diseño de la topología después de la implementación:



Configuración de HTTPS y DNS

Para el HTTPS se configuraron 4 páginas personalizadas:

- La primera página simula la apariencia del buscador de Google
- La segunda, es cuando se realiza una búsqueda se despliegan resultados.
- La tercera es la página de inicio de sesión de Facebook
- La cuarta página es un simple "Hola Mundo"



Para el DNS se ocupó del dominio “<https://www.cisco.com>”

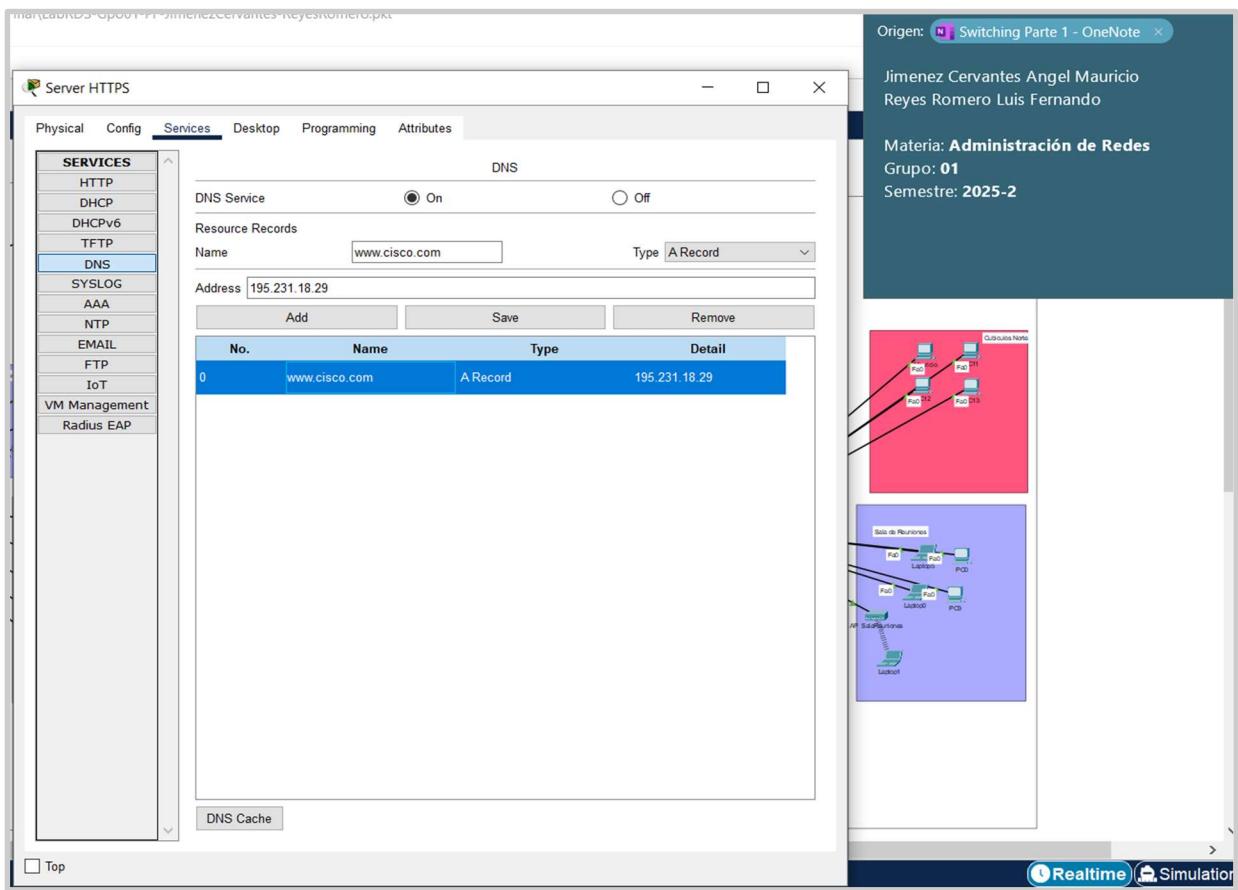


Tabla de enrutamiento

Se empleó el protocolo de enrutamiento OSPF multiárea, a continuación, se muestra la tabla de enrutamiento del Router de Piso 1

The screenshot shows a Cisco Router CLI interface titled "RouterPiso1". The "CLI" tab is selected. The output of the command "sh ip route" is displayed, showing the routing table. The table includes entries for direct connections (Serial0/3/0, FastEthernet0/0, FastEthernet0/1, etc.) and OSPF routes (Area 0, 1, 2). The output also provides route codes and descriptions. To the right of the CLI window is a network diagram titled "Diagrama de Redes" showing various routers (RT_P1, RT_P2, RT_P3) and switches (SW1, SW2, SW3) connected via FastEthernet ports.

```
RT_P1_Enlace(config)#interface FastEthernet0/0
RT_P1_Enlace(config-if)#exit
RT_P1_Enlace(config)#exit
RT_P1_Enlace#
*Apx 14, 10:35:47.3535: SYS-5-CONFIG_I: Configured from console by console
RT_P1_Enlace#
RT_P1_Enlace#
RT_P1_Enlace#
RT_P1_Enlace#
RT_P1_Enlace#
RT_P1_Enlace#
RT_P1_Enlace#
RT_P1_Enlace#sh ip route
Codes: L - local, C - connected, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

      192.169.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.169.1.0/30 is directly connected, Serial0/3/0
L        192.169.1.2/32 is directly connected, Serial0/3/0
      195.231.18.0/24 is variably subnetted, 5 subnets, 3 masks
O  IA    195.231.18.0/27 [110/65] via 192.169.1.1, 4294967295:4294967292:4294967277, Serial0/3/0
O  IA    195.231.18.32/28 [110/65] via 192.169.1.1, 4294967295:4294967292:4294967277, Serial0/3/0
O  IA    195.231.18.48/28 [110/65] via 192.169.1.1, 4294967295:4294967292:4294967277, Serial0/3/0
O  IA    195.231.18.64/28 [110/65] via 192.169.1.1, 4294967295:4294967292:4294967277, Serial0/3/0
O  IA    195.231.18.80/29 [110/65] via 192.169.1.1, 4294967295:4294967292:4294967277, Serial0/3/0
      201.10.1.0/24 is variably subnetted, 8 subnets, 3 masks
C        201.10.1.0/27 is directly connected, FastEthernet0/0.10
L        201.10.1.30/32 is directly connected, FastEthernet0/0.10
C        201.10.1.32/27 is directly connected, FastEthernet0/0.20
L        201.10.1.62/32 is directly connected, FastEthernet0/0.20
C        201.10.1.64/27 is directly connected, FastEthernet0/0.30
L        201.10.1.94/32 is directly connected, FastEthernet0/0.30
C        201.10.1.96/28 is directly connected, FastEthernet0/0.50
L        201.10.1.110/32 is directly connected, FastEthernet0/0.50

RT_P1_Enlace#
```

Mostrando la tabla de enrutamiento del Router de piso 0

RouterPiso0

Physical Config **CLI** Attributes

IOS Command Line Interface

```
*Apr 14, 11:41:11.4141: %IPPHONE-6-REGISTER: ephone-1 IP:195.231.18.66 Socket:2 DeviceType:Phone has registered.  
*Apr 14, 11:41:12.4141: %IPPHONE-6-REGISTER: ephone-4 IP:195.231.18.68 Socket:2 DeviceType:Phone has registered.  
*Apr 14, 10:28:18.2828: %IPPHONE-6-REGISTER: ephone-2 IP:195.231.18.67 Socket:2 DeviceType:Phone has registered.  
  
RT_P0_Enlace>  
RT_P0_Enlace>ena  
Password:  
RT_P0_Enlace#sh ip route  
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP  
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
* - candidate default, U - per-user static route, o - ODR  
P - periodic downloaded static route  
  
Gateway of last resort is not set  
  
192.169.1.0/24 is variably subnetted, 2 subnets, 2 masks  
C     192.169.1.0/30 is directly connected, Serial0/3/0  
L     192.169.1.1/32 is directly connected, Serial0/3/0  
195.231.18.0/24 is variably subnetted, 10 subnets, 4 masks  
C     195.231.18.0/27 is directly connected, FastEthernet0/0.99  
L     195.231.18.30/32 is directly connected, FastEthernet0/0.99  
C     195.231.18.32/28 is directly connected, FastEthernet0/0.10  
L     195.231.18.46/32 is directly connected, FastEthernet0/0.10  
C     195.231.18.48/28 is directly connected, FastEthernet0/0.20  
L     195.231.18.62/32 is directly connected, FastEthernet0/0.20  
C     195.231.18.64/28 is directly connected, FastEthernet0/0.50  
L     195.231.18.78/32 is directly connected, FastEthernet0/0.50  
C     195.231.18.80/29 is directly connected, FastEthernet0/0.30  
L     195.231.18.86/32 is directly connected, FastEthernet0/0.30  
201.10.1.0/24 is variably subnetted, 4 subnets, 2 masks  
O IA   201.10.1.0/27 [110/65] via 192.169.1.2, 4294967295:4294967253, Serial0/3/0  
O IA   201.10.1.32/27 [110/65] via 192.169.1.2, 4294967295:4294967253, Serial0/3/0  
O IA   201.10.1.64/27 [110/65] via 192.169.1.2, 4294967295:4294967253, Serial0/3/0  
O IA   201.10.1.96/28 [110/65] via 192.169.1.2, 4294967295:4294967253, Serial0/3/0  
  
RT_P0_Enlace#
```

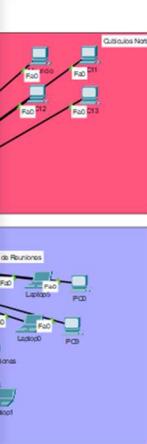
Top

Copy Paste

Origen: 

Jimenez Cervantes Angel Mauricio
Reyes Romero Luis Fernando

Materia: **Administración de Redes**
Grupo: **01**
Semestre: **2025-2**



Ping entre dispositivos finales

Para esta sección se realizarán varias pruebas.

Ping entre PC7(195.231.18.1) que se ubica en la red de administración de piso 0 hacia la PC_Recepción (195.231.18.84) que está en la red de recepción de forma inalámbrica del piso 0.

The screenshot shows a Windows desktop environment. On the left, there is a window titled "PC7" containing a "Command Prompt". The command prompt displays network configuration details and two ping operations. The first ping is to the local IP 195.231.18.84, which fails with a "Request timed out" message. The second ping is to the IP 195.231.18.84, which succeeds with a 0% loss rate. On the right side of the screen, there is a "OneNote" note card with the following information:

Origen: Switching Parte 1 - OneNote

Jimenez Cervantes Angel Mauricio
Reyes Romero Luis Fernando

Materia: **Administración de Redes**
Grupo: **01**
Semestre: **2025-2**

```
Connection-specific DNS Suffix..:
Link-local IPv6 Address.....: FE80::20B:BEFF:FE45:C0C0
IPv6 Address.....: ::
IPv4 Address.....: 195.231.18.1
Subnet Mask.....: 255.255.255.224
Default Gateway.....: ::1
                                         195.231.18.30

Bluetooth Connection:

Connection-specific DNS Suffix..:
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::1
                                         0.0.0.0

C:\>ping 195.231.18.84

Pinging 195.231.18.84 with 32 bytes of data:

Request timed out.
Reply from 195.231.18.84: bytes=32 time=39ms TTL=127
Reply from 195.231.18.84: bytes=32 time=38ms TTL=127
Reply from 195.231.18.84: bytes=32 time=19ms TTL=127

Ping statistics for 195.231.18.84:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 39ms, Average = 32ms

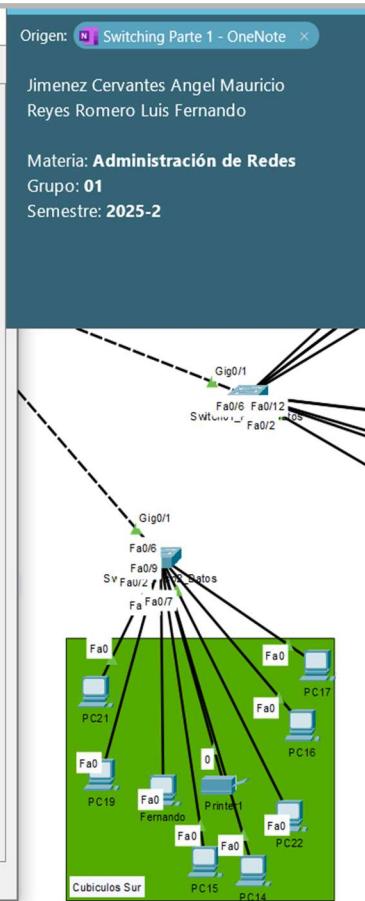
C:\>ping 195.231.18.84

Pinging 195.231.18.84 with 32 bytes of data:

Reply from 195.231.18.84: bytes=32 time=31ms TTL=127
Reply from 195.231.18.84: bytes=32 time=2ms TTL=127
Reply from 195.231.18.84: bytes=32 time=32ms TTL=127
Reply from 195.231.18.84: bytes=32 time=32ms TTL=127

Ping statistics for 195.231.18.84:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

Ping entre PC8(195.231.18.39) que se ubica en la red de área común de piso 0 hacia la PC Fernando (201.10.1.34) que está en la red de Cubículos Sur del Piso 1



The network diagram illustrates a ping from PC8 (195.231.18.39) to PC Fernando (201.10.1.34). PC8 is connected to a switch via port Fa0/6. The switch is also connected to a server (Sv) and several ports labeled Fa0/6 through Fa0/12. A dashed line connects PC8 to a green area representing the 'Cubiculos Sur' floor. Inside this area, PC Fernando is connected to a hub (0) which is further connected to PC15, PC14, and a printer. Other PCs in the area include PC16, PC17, PC18, PC19, and PC22.

```

PC8
Physical Config Desktop Programming Attributes
Command Prompt
Link-local IPv6 Address.....: FE80::2D0:97FF:FE73:8BAE
IPv6 Address.....: ::195.231.18.39
IPv4 Address.....: 195.231.18.39
Subnet Mask.....: 255.255.255.240
Default Gateway.....: ::195.231.18.46

Bluetooth Connection:

Connection-specific DNS Suffix.: 
Link-local IPv6 Address.....: ::1
IPv6 Address.....: ::1
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::1
0.0.0.0

C:\>ping 201.10.1.34
Pinging 201.10.1.34 with 32 bytes of data:
Request timed out.
Reply from 201.10.1.34: bytes=32 time=21ms TTL=126
Reply from 201.10.1.34: bytes=32 time=1ms TTL=126
Reply from 201.10.1.34: bytes=32 time=11ms TTL=126

Ping statistics for 201.10.1.34:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 21ms, Average = 11ms

C:\>ping 201.10.1.34
Pinging 201.10.1.34 with 32 bytes of data:
Reply from 201.10.1.34: bytes=32 time=23ms TTL=126
Reply from 201.10.1.34: bytes=32 time=2ms TTL=126
Reply from 201.10.1.34: bytes=32 time=1ms TTL=126
Reply from 201.10.1.34: bytes=32 time=1ms TTL=126

Ping statistics for 201.10.1.34:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 23ms, Average = 6ms
  
```

Top

Ping entre PC0(201.10.1.69) que se ubica en la red de Sala de Reuniones de piso 1 hacia la PC Sandra (195.231.18.3) que está en la red de Administración del Piso 0

The screenshot shows a Cisco Packet Tracer simulation interface. On the left, a window titled "PC0" displays a Command Prompt session. The session shows the output of the ipconfig command, listing network connections, IP addresses, and subnet masks. It then performs a ping to 195.231.18.3, displaying four successful replies with round-trip times. On the right, a sidebar provides student information: Jimenez Cervantes Angel Mauricio, Reyes Romero Luis Fernando, Materia: Administración de Redes, Grupo: 01, and Semestre: 2025-2. Below the sidebar, a network diagram shows two nodes: PC0 and PC Sandra, connected by a link.

```
Cisco Packet Tracer PC Command Line 1.0
C:>ipconfig

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix.:
Link-local IPv6 Address.....: FE80::202:4AFF:FE61:B11D
IPv6 Address.....: :::
IPv4 Address.....: 201.10.1.69
Subnet Mask.....: 255.255.255.224
Default Gateway.....: :::
201.10.1.94

Bluetooth Connection:

Connection-specific DNS Suffix.:
Link-local IPv6 Address.....: :::
IPv6 Address.....: :::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: :::
0.0.0.0

C:>ping 195.231.18.3

Pinging 195.231.18.3 with 32 bytes of data:

Reply from 195.231.18.3: bytes=32 time=66ms TTL=126
Reply from 195.231.18.3: bytes=32 time=13ms TTL=126
Reply from 195.231.18.3: bytes=32 time=15ms TTL=126
Reply from 195.231.18.3: bytes=32 time=14ms TTL=126

Ping statistics for 195.231.18.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 66ms, Average = 27ms

C:>
```

Asignación de IP's mediante DHCP

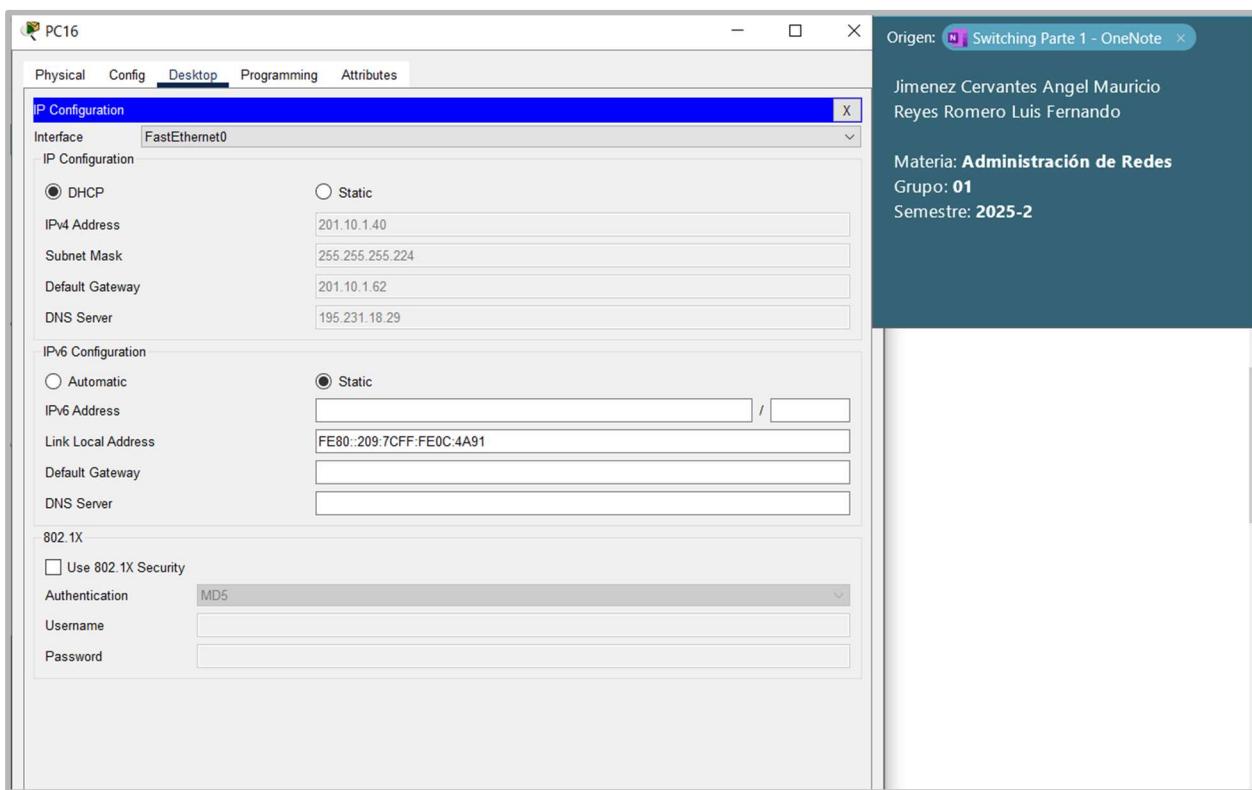
Se mostrarán 3 ejemplos de direcciones IP asignadas por DHCP, pero primero se mostrarán las direcciones IP repartidas en ambos pisos.

Router Piso 0

The screenshot shows a Windows desktop with two main windows. On the left is a terminal window titled "RouterPiso0" displaying the output of the command "sh ip dhcp binding". The output is a table with columns: IP address, Client-ID/, Hardware address, Lease expiration, and Type. Most entries show an IP address starting with 195 or 201, a client ID, a hardware address, a lease expiration of "--", and a type of "Automatic". On the right is a Microsoft OneNote page titled "Switching Parte 1 - OneNote". It contains student information: Jimenez Cervantes Angel Mauricio and Reyes Romero Luis Fernando. Below that are course details: Materia: Administración de Redes, Grupo: 01, and Semestre: 2025-2. At the bottom of the OneNote page is a network diagram showing a switch labeled "Switch PT-Bmpt...ch01/Piso1_Dis" connected to three ports: Gig1/1, Gig2/1, and Gig3. A green shaded area covers the first two ports, and an orange shaded area covers the third port.

IP address	Client-ID/ Hardware address	Lease expiration	Type
195.231.18.1	000B.BE45.C0C0	--	Automatic
195.231.18.3	0050.0F71.4E64	--	Automatic
195.231.18.5	00D0.FFA5.DBDE	--	Automatic
195.231.18.6	0001.43B2.8957	--	Automatic
195.231.18.33	0000.0C5C.4DD6	--	Automatic
195.231.18.35	0002.4AA5.560C	--	Automatic
195.231.18.34	00D0.FF13.9B66	--	Automatic
195.231.18.37	00D0.FFED.3D96	--	Automatic
195.231.18.39	000D.BDD5.8544	--	Automatic
195.231.18.50	0001.C91C.580D	--	Automatic
195.231.18.51	0002.179D.BA13	--	Automatic
195.231.18.52	0010.11D6.2D72	--	Automatic
195.231.18.54	0090.0C2D.02CB	--	Automatic
195.231.18.66	0000.0C8E.7DBD	--	Automatic
195.231.18.65	00E0.8F4A.BA0C	--	Automatic
195.231.18.67	0060.4782.3047	--	Automatic
195.231.18.68	0005.5EB7.CED1	--	Automatic
195.231.18.81	00D0.BA9E.7716	--	Automatic
195.231.18.82	00D0.BCE6.8092	--	Automatic
195.231.18.83	00D0.BA27.85D8	--	Automatic
201.10.1.1	0006.2A06.91CE	--	Automatic
201.10.1.3	0002.4AD1.A0E5	--	Automatic
201.10.1.4	00E0.F7AC.5D88	--	Automatic
201.10.1.5	00E0.F985.E013	--	Automatic
201.10.1.35	0001.C74D.6654	--	Automatic
201.10.1.34	00D0.FF13.C090	--	Automatic
201.10.1.38	0001.421B.7C10	--	Automatic
201.10.1.33	0001.9744.76B9	--	Automatic
201.10.1.37	00D0.5868.25A4	--	Automatic
201.10.1.36	0050.0F1A.0B73	--	Automatic
201.10.1.40	0009.7C0C.4A91	--	Automatic
201.10.1.39	00D0.97BB.7381	--	Automatic
201.10.1.41	00D0.D3DC.3A07	--	Automatic
201.10.1.65	0001.C945.AB70	--	Automatic
201.10.1.66	0002.4A61.B11D	--	Automatic
201.10.1.68	0002.4AB9.BA5B	--	Automatic
201.10.1.67	0000.0C9E.92A5	--	Automatic
201.10.1.69	0005.5E4C.A6EB	--	Automatic

Mostrando la PC16

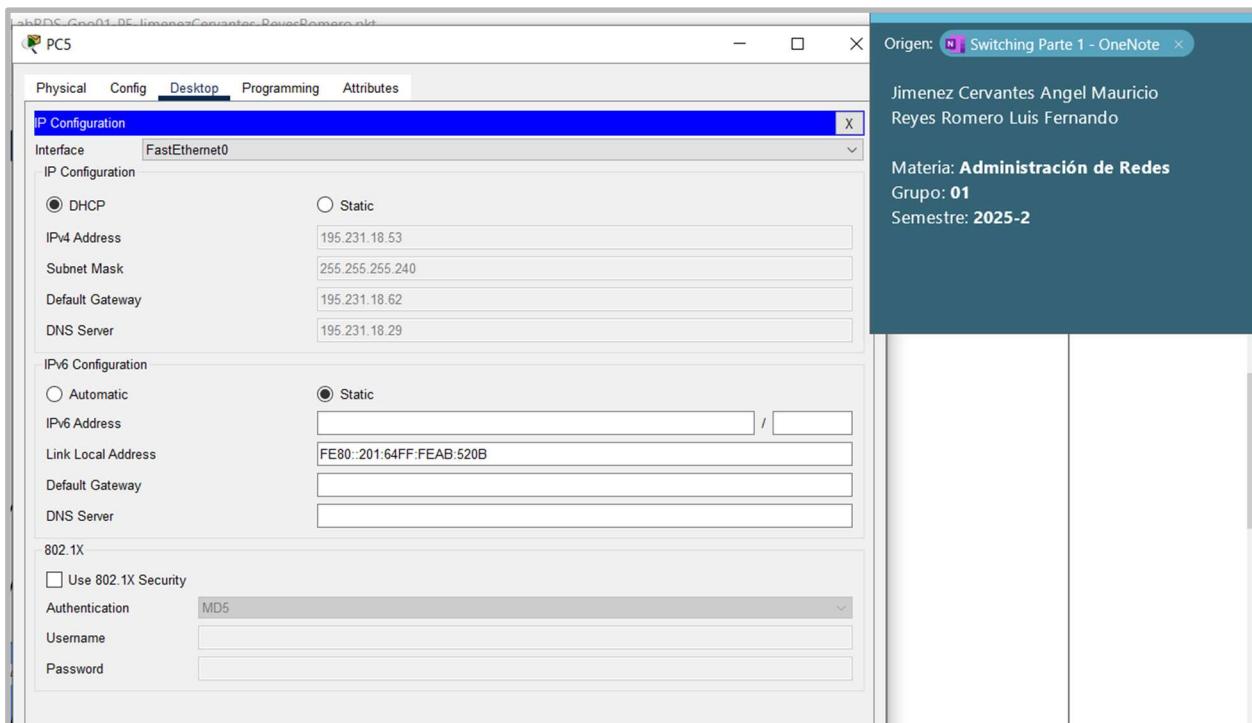


Origen: Switching Parte 1 - OneNote

Jimenez Cervantes Angel Mauricio
Reyes Romero Luis Fernando

Materia: Administración de Redes
Grupo: 01
Semestre: 2025-2

Mostrando la PC5

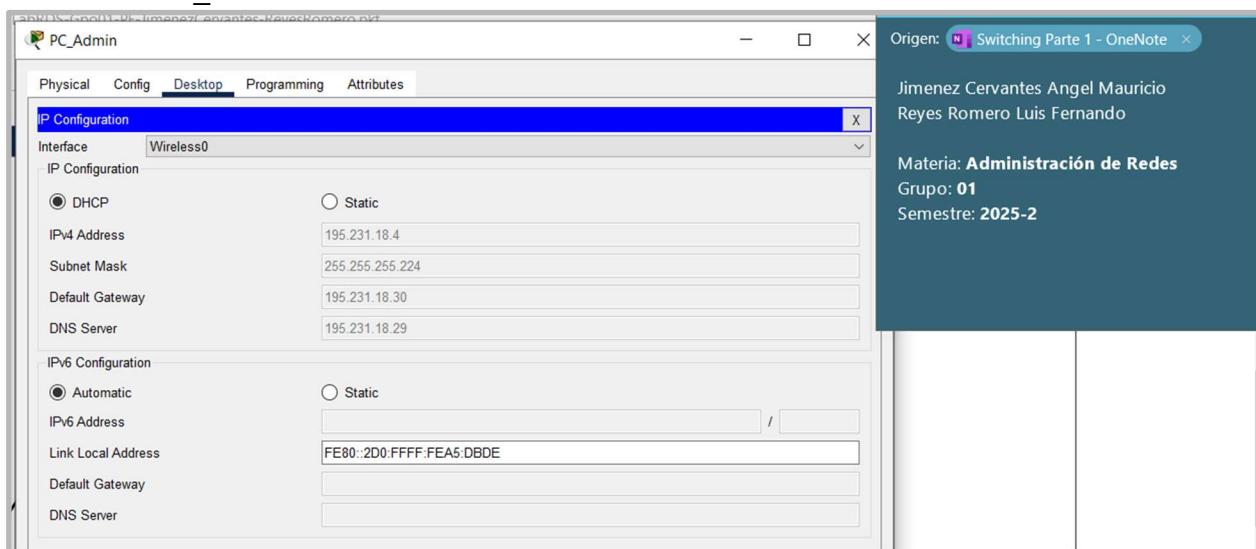


Origen: Switching Parte 1 - OneNote

Jimenez Cervantes Angel Mauricio
Reyes Romero Luis Fernando

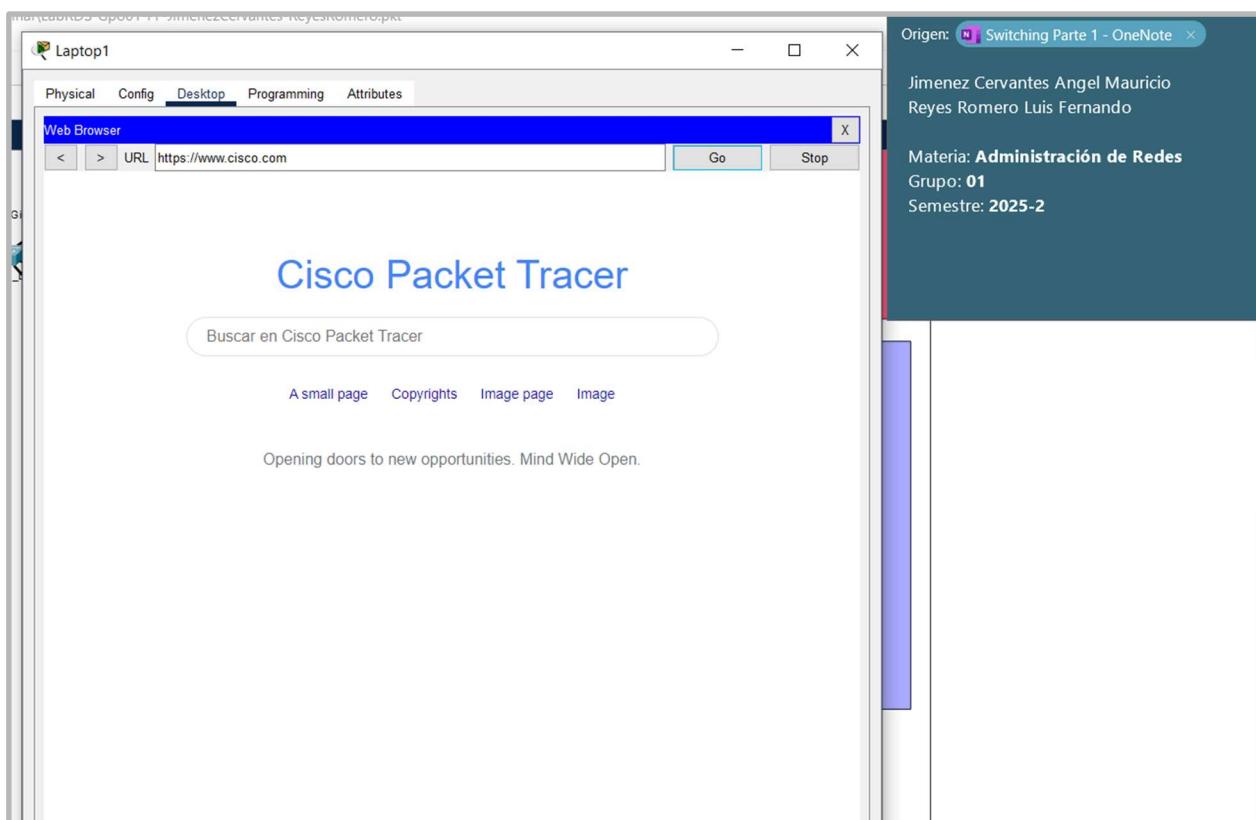
Materia: Administración de Redes
Grupo: 01
Semestre: 2025-2

Mostrando PC_Admin

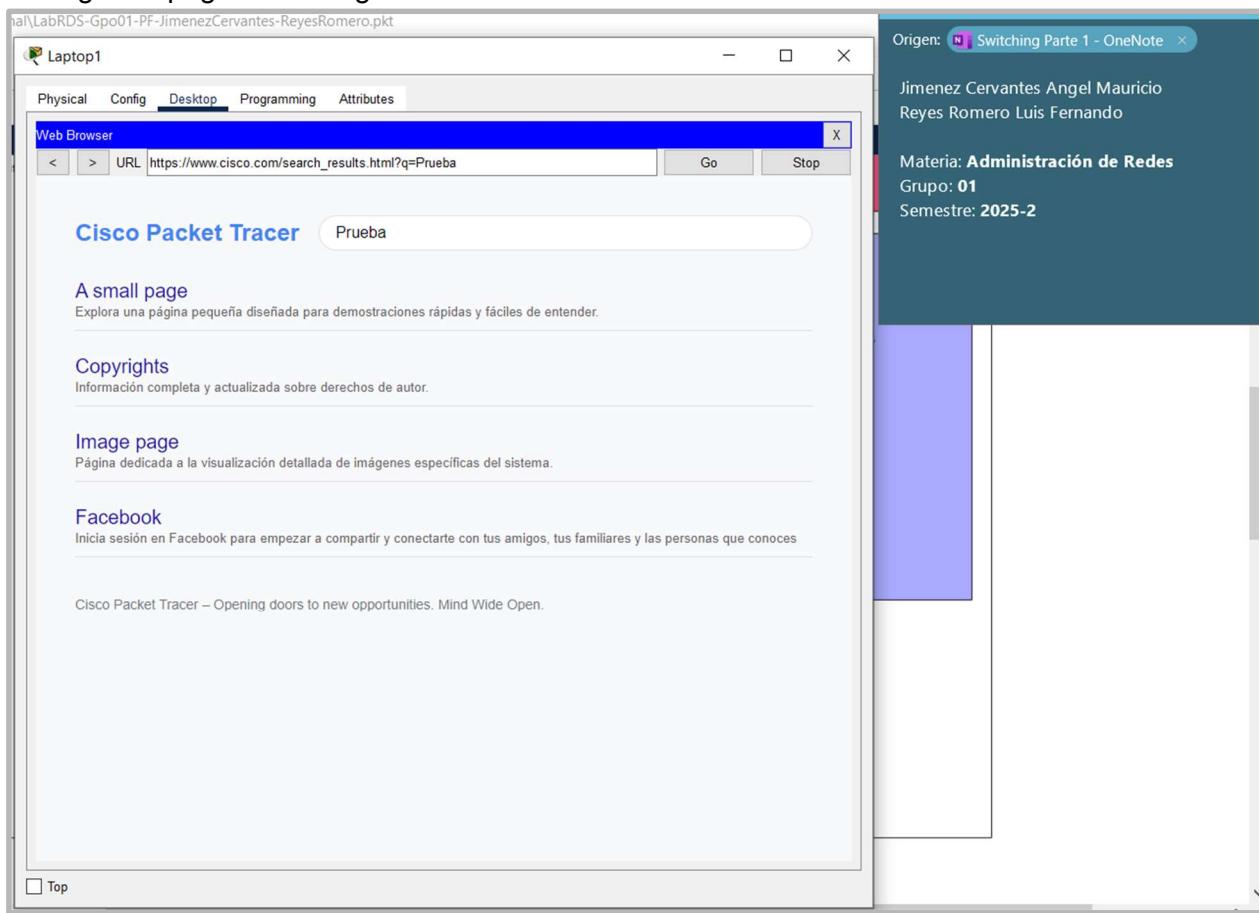


Demostración del Sitio web personalizado

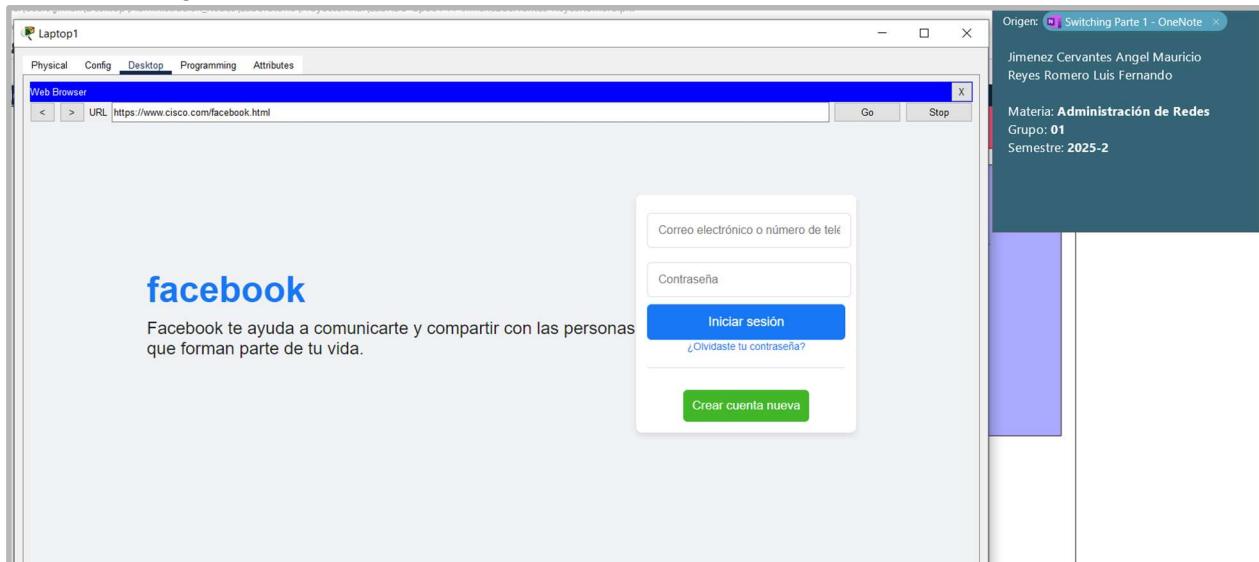
Para acceder al sitio web usaremos el dominio “<https://www.cisco.com>” para acceder usaremos la Laptop 1, la primera página luce así:



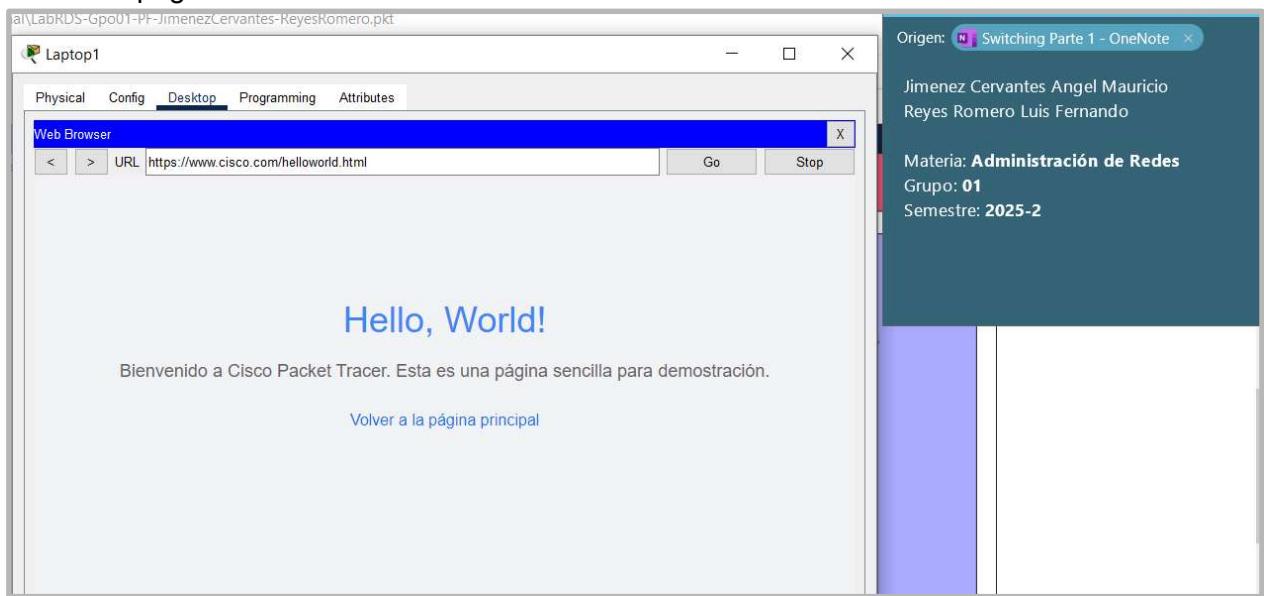
La segunda página es la siguiente:



La tercera página es:



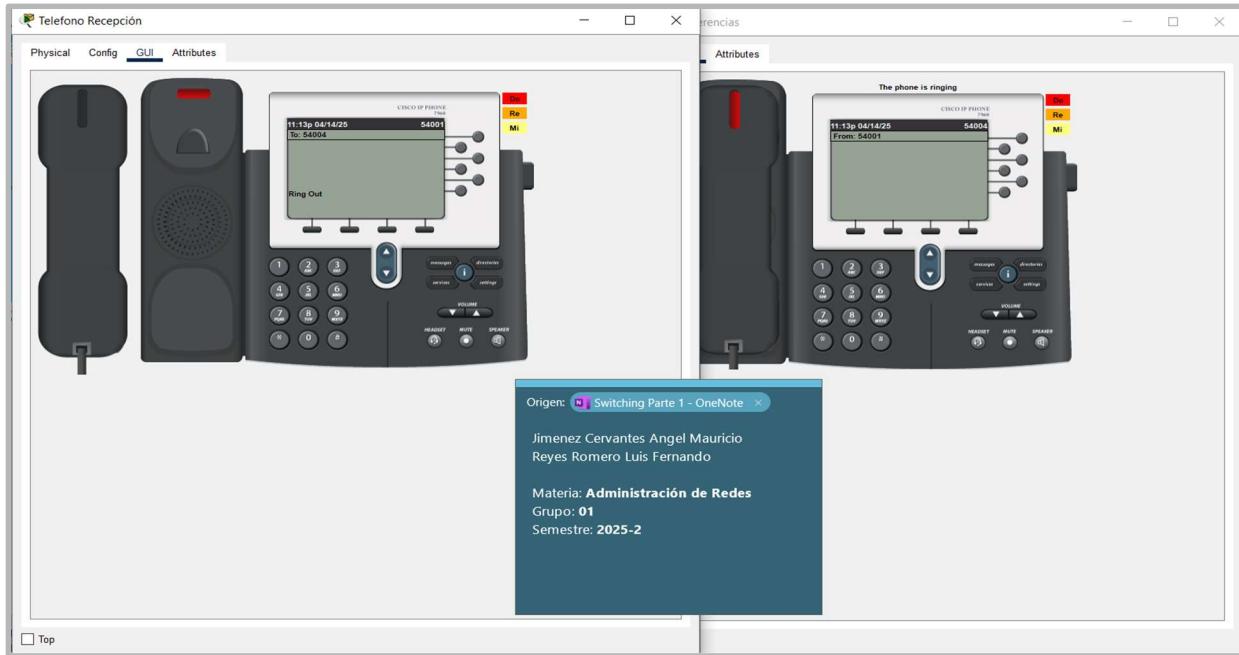
La cuarta página es:



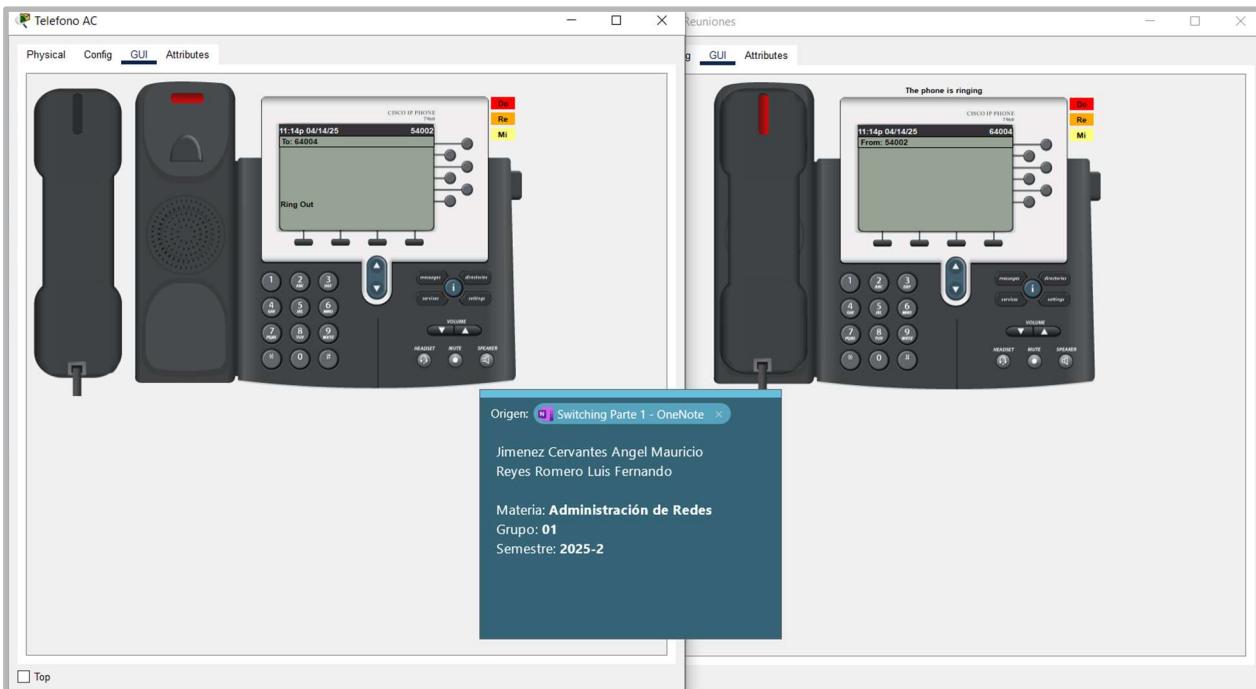
Demostración del Servicio de VoIP

Para el piso 0 se usó la extensión 5400X y para el piso 1 la extensión 6400X a continuación se realizarán varias pruebas

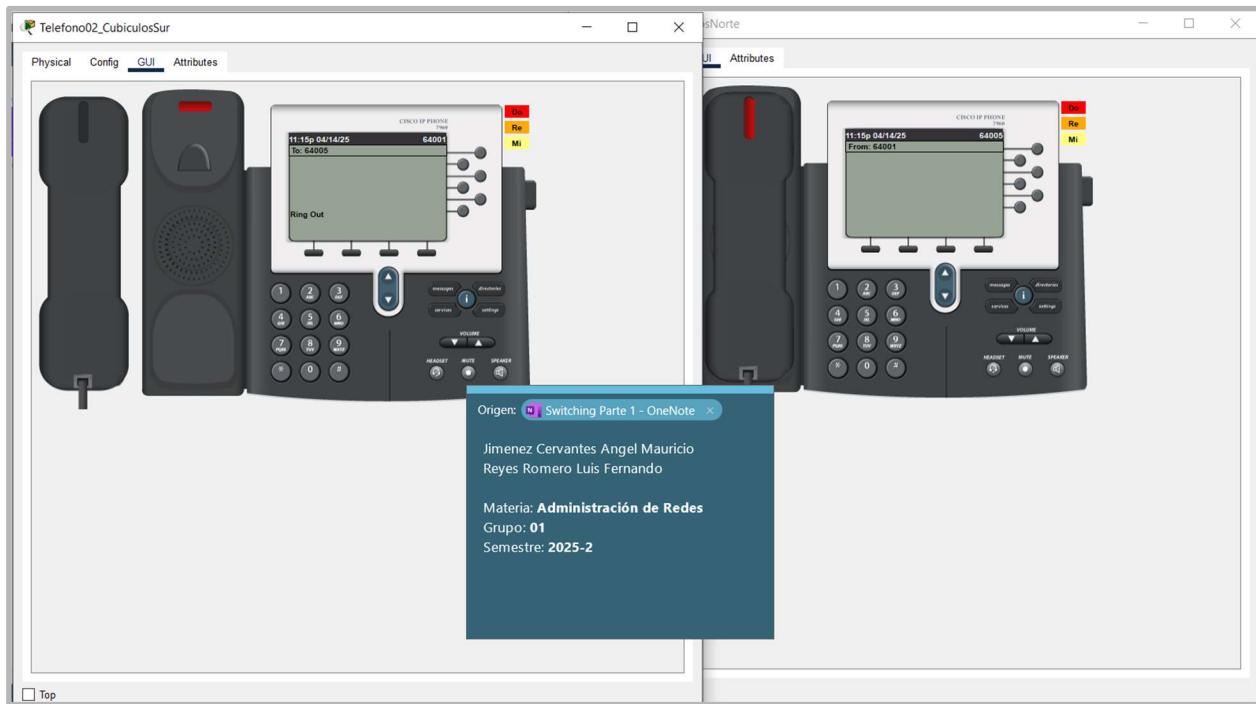
De la extensión 54001 a 54004



De la extensión 54002 a 64004

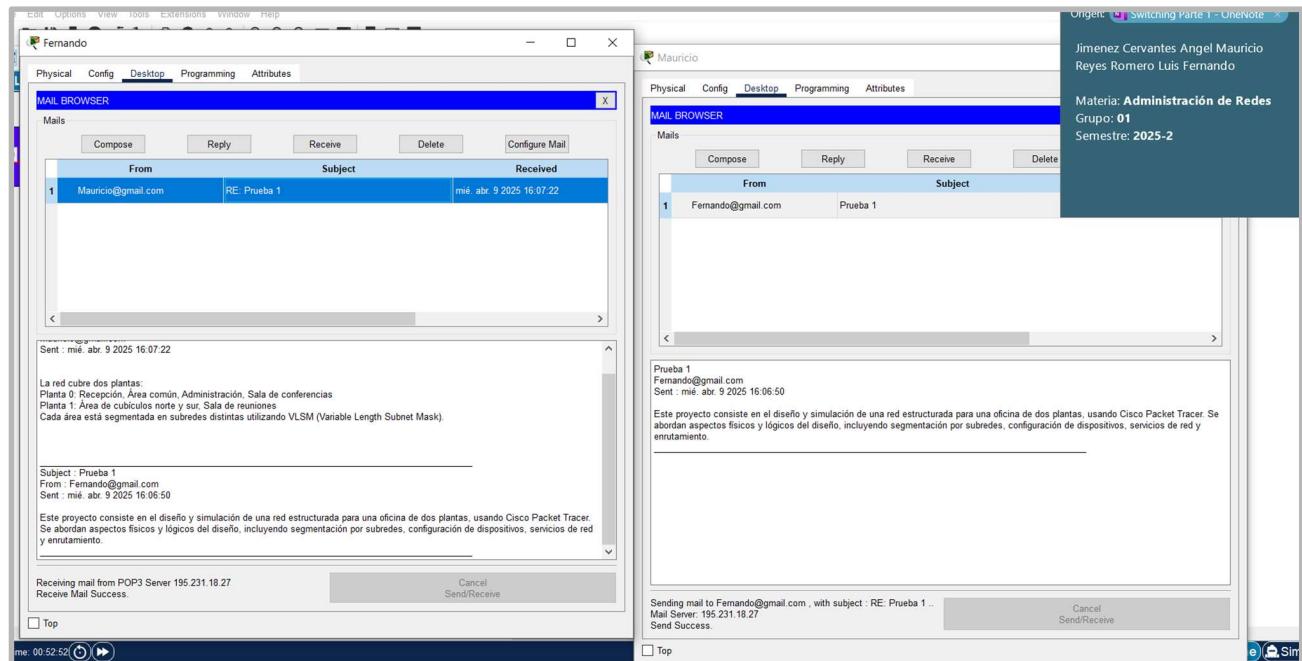


De la extensión 64001 a 64005



Demostración del funcionamiento del servidor de correo

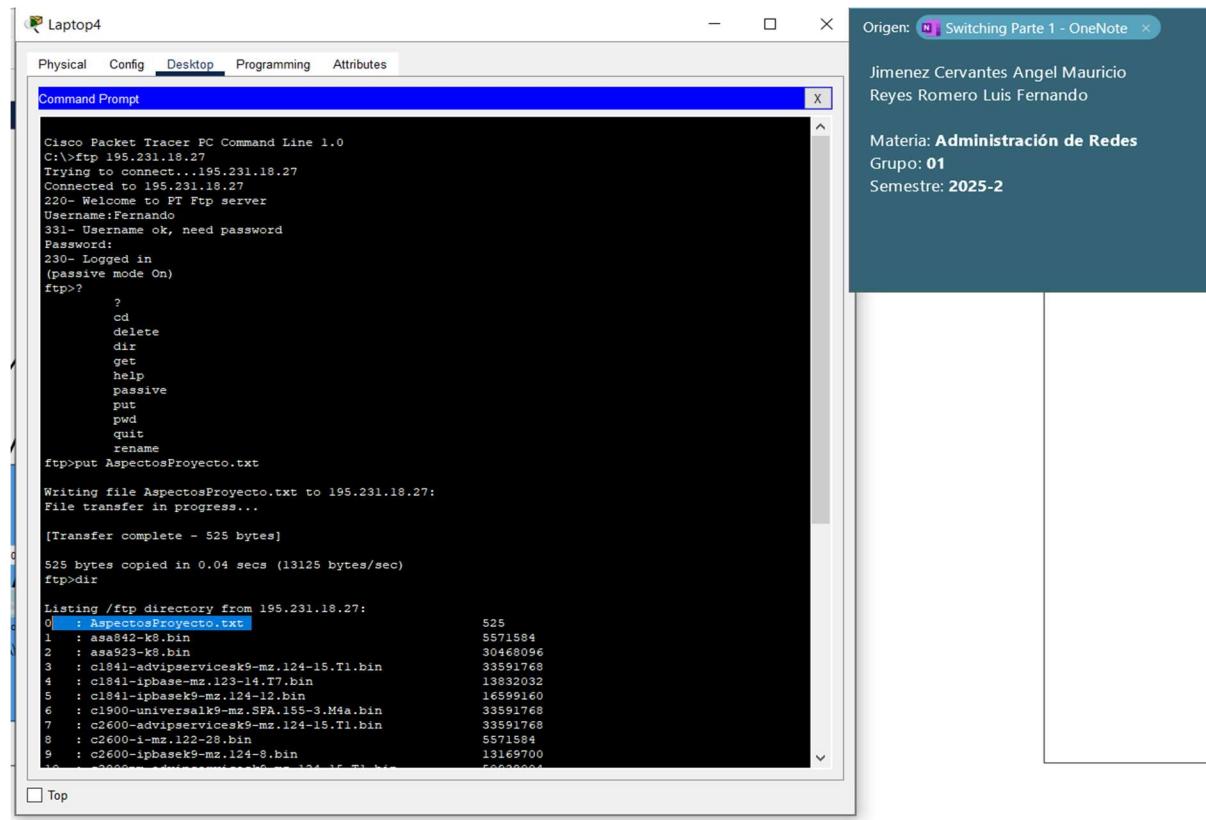
Se realizará el envío desde el correo de la PC Fernando a PC Mauricio y se responderán entre sí



Demostración del funcionamiento del servidor de ftp

Subiremos un archivo llamado AspectosProyecto.txt desde la Laptop4 y se descargara en la PC19

Primero la subida del archivo:



The screenshot shows a Cisco Packet Tracer window titled "Laptop4". Inside, a "Command Prompt" window is open. The command line shows the following session:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 195.231.18.27
Trying to connect...195.231.18.27
Connected to 195.231.18.27
220- Welcome to PT Ftp server
Username:Fernando
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>?
?
cd
delete
dir
get
help
passive
put
pwd
quit
rename
ftp>put AspectosProyecto.txt
Writing file AspectosProyecto.txt to 195.231.18.27:
File transfer in progress...
[Transfer complete - 525 bytes]
525 bytes copied in 0.04 secs (13125 bytes/sec)
ftp>dir
Listing /ftp directory from 195.231.18.27:
0 : AspectosProyecto.txt      525
1 : asa842-k8.bin      5571584
2 : asa923-k8.bin      30468096
3 : c1841-advp�servicesk9-mz.124-15.T1.bin 33591768
4 : c1841-ipbasek9-mz.123-14.17.bin 13832032
5 : c1841-ipbasek9-mz.124-12.bin 16599160
6 : c1900-universalk9-mz.5PA.155-3.Mda.bin 33591768
7 : c2600-advp�servicesk9-mz.124-15.T1.bin 33591768
8 : c2600-1-mz.122-28.bin 5571584
9 : c2600-ipbasek9-mz.124-8.bin 13169700
10 : c2600-universalk9-mz.5PA.155-3.Mda.bin 56698064
```

To the right of the terminal window, there is a OneNote note card with the following information:

Origen: Switching Parte 1 - OneNote

Jimenez Cervantes Angel Mauricio
Reyes Romero Luis Fernando

Materia: Administración de Redes
Grupo: 01
Semestre: 2025-2

Después la descarga en la PC19

The screenshot shows a Windows desktop environment. On the left, there is a Command Prompt window titled "Command Prompt". The window displays a session of an FTP client connecting to a server at 195.231.18.27. The user logs in as "Mauricio" and downloads a file named "AspectosProyecto.txt". After the download, the user attempts to run the file, which results in an error message: "Invalid or non supported command." The user then exits the FTP session. On the right side of the screen, there is a OneNote note card with the following information:

Origen: Switching Parte 1 - OneNote

Jimenez Cervantes Angel Mauricio
Reyes Romero Luis Fernando

Materia: Administración de Redes
Grupo: 01
Semestre: 2025-2

Demostración de SSH a los routers

Para acceder a los routers usaremos la PC7.

De PC7 a Router Piso 0

```
C:\>
C:\>
C:\>
C:\>
C:\>ssh -l admin 192.169.1.1

Password:
RT_P0_Enlace>ena
Password:
RT_P0_Enlace#sh run
Building configuration...

Current configuration : 3548 bytes
!
version 15.1
service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname RT_P0_Enlace
!
!
!
enable secret 5 $1$0mERr$IiuNiacV1BVdIKbrjvWYU0
!
!
ip dhcp excluded-address 195.231.18.61
ip dhcp excluded-address 195.231.18.28
ip dhcp excluded-address 195.231.18.45
ip dhcp excluded-address 195.231.18.77
ip dhcp excluded-address 195.231.18.29
ip dhcp excluded-address 195.231.18.27
ip dhcp excluded-address 195.231.18.20
ip dhcp excluded-address 195.231.18.26
ip dhcp excluded-address 195.231.18.25
ip dhcp excluded-address 195.231.18.22
ip dhcp excluded-address 195.231.18.23
ip dhcp excluded-address 195.231.18.24
!
ip dhcp pool administracion
  network 195.231.18.0 255.255.255.224
  default-router 195.231.18.30
  dns-server 195.231.18.29
  ip dhcp pool areaComun
    network 195.231.18.32 255.255.255.240
```

Origen: Switching Parte 1 - OneNote

Jimenez Cervantes Angel Mauricio
Reyes Romero Luis Fernando

Materia: **Administración de Redes**
Grupo: **01**
Semestre: **2025-2**

De PC7 a Router Piso 1

The screenshot shows a Windows desktop environment. On the left, there is a Command Prompt window titled "PC7" with the following content:

```
C:\>
C:\>ssh -l admin 192.169.1.2
Password:
RT_Pl_Enlace>
RT_Pl_Enlace>ena
Password:
RT_Pl_Enlace#SH RUN
Building configuration...

Current configuration : 3184 bytes
!
version 15.1
service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname RT_Pl_Enlace
!
!
enable secret 5 $1$mERr$IiuNiaoV1BVdlKbrjvWYU0
!
ip dhcp excluded-address 201.10.1.29
ip dhcp excluded-address 201.10.1.93
ip dhcp excluded-address 201.10.1.61
ip dhcp excluded-address 201.10.1.109
!
ip dhcp pool VoIP_Piso1
network 201.10.1.96 255.255.255.240
default-router 201.10.1.110
option 150 ip 201.10.1.110
dns-server 195.231.18.29
ip dhcp pool CubiculosNorte
network 201.10.1.0 255.255.255.224
default-router 201.10.1.30
dns-server 195.231.18.29
ip dhcp pool CubiculosSur
network 201.10.1.32 255.255.255.224
default-router 201.10.1.62
dns-server 195.231.18.29
ip dhcp pool SalaReuniones
network 201.10.1.64 255.255.255.224
default-router 201.10.1.94
```

On the right side of the screen, there is a OneNote note card with the following information:

Origen: Switching Parte 1 - OneNote

Jimenez Cervantes Angel Mauricio
Reyes Romero Luis Fernando

Materia: **Administración de Redes**
Grupo: **01**
Semestre: **2025-2**

Demostración de telnet a switches

Haremos uso de la PC21 para realizar los telnet

De PC21 hacia el Switch Distribucion Piso 0

The screenshot shows a Cisco Packet Tracer window titled "Command Prompt". The window displays the configuration of a Cisco switch via Telnet. The configuration includes:

```
Cisco Packet Tracer PC Command Line 1.0
C:>telnet 195.231.18.61
Trying 195.231.18.61 ...Open

User Access Verification

Username: admin
Password:
SW_P0_Distribucion>ena
Password:
Password:
SW_P0_Distribucion#SH RUN
Building configuration...

Current configuration : 1127 bytes
!
version 12.1
service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW_P0_Distribucion
!
enable secret 5 $1$ERr$IiuNiaoVlBVdlKbrjvWYU0
!
!
!
username admin secret 5 $1$ERr$TbHullN28cEp8lkLqr0f/
!
ip dhcp snooping vlan 10,20,30,50,99
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface GigabitEthernet0/1
 ip dhcp snooping trust
 switchport mode trunk
!
interface GigabitEthernet1/1
!
```

To the right of the terminal window, there is a OneNote note with the following information:

Origen: Switching Parte 1 - OneNote

Jimenez Cervantes Angel Mauricio
Reyes Romero Luis Fernando

Materia: Administración de Redes
Grupo: 01
Semestre: 2025-2

De PC21 hacia el Switch VoIP Piso 1

The screenshot shows a Windows desktop environment. On the left is a Command Prompt window titled "PC21" with the following text:

```
* Connection timed out, remote host not responding
C:\telnet 201.10.1.109
Trying 201.10.1.109 ...Open

User Access Verification

Username: admin
Password:
% Login invalid

Username: admin
Password:
SW_Pl_VoIP>ena
Password:
SW_Pl_VoIP#
SW_Pl_VoIP#SH RUN
Building configuration...

Current configuration : 2044 bytes
!
version 15.0
service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW_Pl_VoIP
!
enable secret 5 $1$mERr$IiuNiaoViBVd1KbrjvWYUO
!
!
!
username admin secret 5 $1$mERr$yTbHullN28cEp8lkLqrOf/
!
!
ip dhcp snooping vlan 50
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 ip dhcp snooping trust
 switchport mode access
 switchport voice vlan 50
```

To the right of the Command Prompt is a OneNote note card with the following information:

Origen: **Switching Parte 1 - OneNote**

Jimenez Cervantes Angel Mauricio
Reyes Romero Luis Fernando

Materia: **Administración de Redes**
Grupo: **01**
Semestre: **2025-2**

Conclusiones

Este proyecto sobre el cableado estructurado para el edificio de oficinas ha sido diseñado con el objetivo de proporcionar una infraestructura de red robusta, eficiente y escalable, que soporte tanto la comunicación de datos como de voz de manera óptima. A través de un análisis de los requerimientos y factibilidad, se ha determinado que el uso de cables directos y cruzados junto con una topología jerárquica, garantizamos un rendimiento adecuado y la capacidad de una expansión futura.

Algunos de los beneficios de este proyecto son: que garantizamos la continuidad operativa de las comunicaciones en la empresa, mejora la velocidad de transmisión de datos, y reduce los costos asociados con fallos de red. Además, su diseño permite adaptarse a las necesidades cambiantes de la infraestructura, facilitando futuras ampliaciones o modificaciones sin grandes intervenciones.

A futuro, el sistema de cableado estructurado propuesto se adapta perfectamente a las demandas de una empresa en crecimiento, permitiendo una integración eficiente de nuevas tecnologías o servicios y un mantenimiento sencillo. Este enfoque asegura que la red sea sostenible a largo plazo, respaldando tanto las operaciones diarias de la organización como su evolución tecnológica en el tiempo. Con esta infraestructura, la empresa estará mejor preparada para afrontar los desafíos de un entorno de trabajo cada vez más digitalizado.

Referencias

- A, Cristian (2023, 6 noviembre). *Cableado estructurado, qué es, tipos y utilidades.* Redes & Telecom. <https://www.redestelecom.es/infraestructuras/cableado-estructurado-que-es-tipos-y-utilidades/>
- Data Mercantil. (S/F). *¿Qué es el Cableado Estructurado? Definición, Características, Componentes y Normas.* <https://datamercantil.com/que-es-el-cableado-estructurado/>
- Enreach. (2021, junio 10). *¿Qué necesitas para utilizar la telefonía VoIP en tu empresa?.* <https://enreach.es/blog/que-necesitas-para-utilizar-voip/>
- Fernández, Y. (2019, octubre 12). *VoIP: qué es y cómo funciona.* Xataka. <https://www.xataka.com/basics/voip-que-como-funciona>
- Networking Basics - Skills for all. (S/F). <https://www.netacad.com/course/ccna-switching-routing-wireless-essentials>
- Rodrigo. (2021, agosto 07). *¿Cuál es la diferencia entre cable de red directo y cable de red cruzado?.* FS. <https://www.fs.com/es/blog/patch-cable-vs-crossover-cable-what-is-the-difference-4767.html>
- Walton, A. (2018, enero 25). *Configuración de OSPF Multiárea.* CCNA Desde Cero. <https://ccnadesdecero.es/configuracion-de-ospf-multiarea/>
- Walton, A. (2020, January 12). *DHCP (Dynamic Host Configuration Protocol).* CCNA Desde Cero. <https://ccnadesdecero.es/dhcp-dynamic-host-configuration-protocol/>
- Walton, A. (2018, enero 30). *Diseño Jerárquico de Redes.* CCNA Desde Cero. <https://ccnadesdecero.es/diseno-jerarquico-de-redes/>

Walton, A. (2018, febrero 06). *syslog: Funcionamiento y Configuración*. CCNA Desde Cero. <https://ccnadesdecero.es/syslog-funcionamiento-y-configuracion/>